

EDITAL – PE Nº 005/2026
Processo Administrativo nº 26/049-00
Processo SEI Nº 065.10933.2026.0003946-61

EDITAL

- (X) PREGÃO ELETRÔNICO Nº 005/2026
(X) SISTEMA DE REGISTRO DE PREÇOS

PREÂMBULO

1. Regência legal:

Esta licitação obedecerá às disposições da Constituição Federal, da Lei Federal nº 13.303 de 30 de junho de 2016, da Lei Complementar nº 123/06 e suas alterações, do Regulamento de Licitações e Contratos da PRODEB, disponível para acesso através do link: <https://www.ba.gov.br/prodeb/licitacao/regulamento-de-licitacoes-e-contratos>, da Lei Federal nº 14.133/2021, da Lei Estadual nº 14.634/2023, da Lei Federal nº 13.709/2018, do Decreto Estadual nº 22.886/2024, do Decreto Estadual nº 22.888/2024, do Decreto Estadual nº 23.113/2024, do Decreto Estadual nº 23.356/2025, do Decreto Estadual nº 23.657/2025, do Decreto Estadual nº 24.318/2026 e respectivas alterações, quando couber e do Código de Ética e Conduta da PRODEB disponível através do link: <http://www.prodeb.ba.gov.br/documentos%20compartilhados/c%c3%b3digo%20de%20conduta%20e%20integridade%20da%20prodeb.pdf>, bem como da legislação específica.

2. Requisito de participação:

2.1 Inscrição no Cadastro de Fornecedores do Estado da Bahia /SAEB ou no SICAF:

- (x) Serão admitidos a participar desta licitação os interessados, **inscritos ou não** no Cadastro de Fornecedores do Estado da Bahia ou no SICAF, que atenderem a todas as exigências contidas neste instrumento, e que pertençam ao ramo de atividade pertinente ao objeto licitado, e que tenham realizado seu credenciamento como *usuário* junto ao Banco do Brasil, para a obtenção de chave de identificação ou senha individual.

2.2 Tratamento diferenciado e simplificado

- () Participação restrita a Microempresa e Empresa de Pequeno Porte
- (X) Ampla Participação
- () Aquisições
- () Sem reserva de cota
- () Com reserva de cota
- (X) Serviços – Sem reserva de cota
- () Híbrido
- () Itens com participação restrita a Microempresa e Empresa de Pequeno Porte
- () Itens de Ampla Participação
- () Aquisições
- () Sem reserva de cota
- () Com reserva de cota
- () Serviços – Sem reserva de cota
- 2.2.1** A obtenção do benefício a que se refere este subitem 2.2 fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, conforme art. 1º, §3º do RLC/PRODEB e art. 4º, §2º da Lei Federal nº 14.133/2021.

3. Processo administrativo / Setor:

065.10933.2026.0003946-61

PRODEB/DTC

4. Modalidade/número de ordem:

(☒) PREGÃO nº
ELETRÔNICO **005/2026**
BB nº 1092968

4.1 Modo de disputa (☒) Aberto () Aberto e fechado () Fechado e aberto	4.2 Intervalo mínimo de diferença entre lances (degrau de valor ou percentual): (☒) Sim (conforme item 12.7 do Termo de Referência) () Sim () Sim

5. Critério de julgamento:

(☒) Menor Preço	() Por item (☒) Por lote (☒) Global
() Maior Desconto	() Por item () Por lote () Global

(☒) Não será admitida a previsão de preços diferentes em razão de local de entrega ou de acondicionamento, tamanho de lote ou qualquer outro motivo.

5.1 O regime de execução do contrato será empreitada por preço unitário.

6. Objeto da licitação/Codificação no Certificado de Registro:

Implantação de sistema de registro de preços, objetivando a formalização de ata com vencedor do certame, visando a contratação de empresa especializada em solução de conectividade segura, incluindo proteção de borda, firewall de próxima geração, links de internet e solução de operação e monitoramento central, pelo período de 60 meses e soluções de segurança da informação e cibersegurança, compreendendo licenciamento, atualização, garantia e demais serviços associados, pelo período de 12 meses, nos termos e condições previstas no Termo de Referência e seus anexos.

Família/Código:

Conforme item 4 do Termo de Referência.

7. Dotação orçamentária:

As despesas decorrentes da contratação correrão à conta da dotação orçamentária do Contratante, devendo cada contratação ser precedida da emissão da declaração de compatibilidade com a LRF, quando couber.

8. Ordem de fases da licitação:

- (☒) Na presente licitação, a fase de habilitação **sucedará** as fases de apresentação de propostas e lances e de julgamento.
- () Na presente licitação, a fase de habilitação **antecederá** as fases de apresentação de propostas e lances e de julgamento, conforme **ato motivado com explicitação dos benefícios decorrentes**.

9. Vistoria:

- (☒) Não Exigível
- () Exigível

10. Propostas e documentos de habilitação:

10.1 O prazo de validade da proposta será de, no mínimo, 60 (sessenta) dias, a contar da data de sua apresentação.

10.2 O licitante NÃO poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação, obrigando-se nos limites da oferta.

10.3 Os documentos de habilitação do licitante vencedor serão enviados por meio do sistema eletrônico, em formato digital, no prazo 3 (três) horas, prorrogável por igual período, contado da solicitação de encaminhamento dos citados documentos pelo Pregoeiro.

10.3.1 Para fins desse Edital, considera-se responsável pela licitação o Pregoeiro.

11. Critérios específicos:

11.1 Consórcio

11.1.1 Participação de pessoas jurídicas reunidas em consórcio

(☒) Sim

(☐) Não

11.1.2 Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o Termo de Referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo no percentual de 10% (dez por cento) para o consórcio em relação ao valor exigido para os licitantes individuais, conforme item 15.2.7 do Termo de Referência.

11.2 Registro de preços

11.2.1 Abrangência do registro: o âmbito deste registro de preços é o designado abaixo:

- (☒) Estadual – conforme abrangência definida no item 2.3.2, “m” do ETP do Lote 1 e no item 2.3.2, “k” do ETP do Lote 2, a saber:

Lote 1:

- i. Os órgãos e entidades da Administração Pública direta, autárquica e fundacional do Poder Executivo Estadual;
- ii. As empresas públicas e sociedades de economia mista integrantes da Administração Pública indireta, observado o regime jurídico aplicável a cada ente;
- iii. Eventuais órgãos participantes dos Poderes Legislativo e Judiciário, do Tribunal de Contas do Estado, do Tribunal de Contas dos Municípios, do Ministério Público do Estado e da Defensoria Pública do Estado, desde que formalmente indicados como participantes do Sistema de Registro de Preços;
- iv. A adesão de órgãos não participantes, nos termos do art. 86, §2º, da Lei Federal nº 14.133/2021, condicionada à análise e manifestação favorável da Secretaria da Administração – SAEB.

Lote 2:

A Ata de Registro de Preços a ser formada terá abrangência para os órgãos e entidades do Poder Executivo Estadual, permitindo a realização de contratações conforme as necessidades específicas de cada demandante, observados os limites, as condições e os quantitativos registrados.

(☐) Regional, compreendendo a região _____

(☐) Local, compreendendo apenas o município de _____

(☐) Interfederativo

11.3 Adesão posterior à ata de registro de preços (carona):

- (☒) Poderá haver adesão posterior à ata de registro de preços decorrente desta licitação, devendo ser observados os seguintes limites quantitativos e as regras definidas na minuta da ata de registro de preços:
- a) as contratações adicionais não poderão exceder, por órgão ou entidade solicitante, a 50% (cinquenta por cento) dos quantitativos dos itens do edital da licitação, do aviso ou do instrumento de contratação direta, registrados na ata de registro de preços para o órgão ou a entidade gerenciadora e para os órgãos ou as entidades participantes; e
 - b) o quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão ou a entidade gerenciadora e os órgãos ou as entidades participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

() Não poderá haver adesão posterior à ata de registro de preços decorrente desta licitação

12. Disponibilização do Edital, Impugnação e Pedidos de esclarecimentos:

12.1 O Edital e seus Anexos estão disponíveis, na íntegra, no portal *Comprasnet.ba*, no endereço eletrônico www.prodeb.ba.gov.br, no portal do licitações-e do BB, <https://licitacoes-e2.bb.com.br/> e no Portal Nacional de Contratações Públicas – PNCP.

12.2 A impugnação e o pedido de esclarecimento serão realizados por petição ou por mensagem no correio eletrônico: licitacao@prodeb.ba.gov.br.

13. Local, dia e hora para recebimento das propostas e documentos e início da sessão pública da licitação:

Site: <https://licitacoes-e2.bb.com.br/>

Recebimento das propostas: das 08:00 horas do dia 15/05/2026 às 10:00 horas do dia 28/05/2026

Início da sessão pública: às 10:00 horas do dia 28/05/2026

14. Disponibilização dos autos para recurso:

14.1 O licitante deverá solicitar o acesso aos autos, o qual será concedido por meio de envio de *link* para o correio eletrônico (e-mail) cadastrado do usuário externo no Sistema Eletrônico de Informação – SEI.

15. Prazo de vigência da ata de registro de preços:

15.1 O prazo de vigência da ata de registro de preços será de 1 (um) ano, podendo ser prorrogado por igual período, conforme art. 137 do RLC/PRODEB e art. 18 do Decreto Estadual nº 23.657/2025.

16. Prazo para assinatura:

16.1 O(s) fornecedor(es) ou prestador(es) de serviço(s) será(ão) convocado(s) para assinar a Ata de Registro de Preços no prazo de até 05 (cinco) dias úteis, prorrogável por igual período.

16.1.1 O prazo de convocação de que trata o subitem 16.1 poderá ser prorrogado uma vez, por igual período, mediante solicitação do interessado durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela PRODEB.

16.2 O prazo para assinatura do contrato ou retirada do instrumento equivalente será de: 05 (cinco) dias úteis, observado o disposto no art. 167 do RLC da PRODEB.

16.2.1 O prazo de convocação de que trata o subitem 16.2 poderá ser prorrogado uma vez, por igual período, mediante solicitação do Adjudicatário durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela PRODEB.

16.3 A assinatura da ata de registro de preços e do contrato se dará por meio do Sistema Eletrônico de Informações - SEI, caso em que a licitante deverá providenciar o cadastramento de seu representante legal ou procurador no www.portalseibahia.saeb.ba.gov.br ou através do link disponibilizado no endereço eletrônico www.comprasnet.ba.gov.br.

17. Exame prévio da minuta e aprovação da assessoria jurídica:

Declaro que a fase interna deste procedimento foi examinada pelo órgão legal de assessoramento jurídico, conforme o Parecer ASJ de 08 de maio de 2026 (Doc. SEI nº 00139640101).

18. Anexos do Edital:

Constituem partes integrantes deste Edital, como se nele literalmente transcritos, os seguintes anexos:

I. Termo de Referência e Anexos

II. Minuta de Ata de Registro de Preços

III. Minutas de Contratos – PRODEB/ demais Órgãos e Entidades

IV. Modelo de Declaração de Enquadramento (Lei Complementar nº123/06), nos termos do art. 1º, §3º do RLC da PRODEB e art. 4º, §2º da Lei Federal nº 14.133/2021.

V. Modelo de Declaração Unificada

VI. Modelo de Procuração

VII. Modelo de Petição de Impugnação/Recurso

VIII. Modelo de Prova de Qualificação Técnica

19. Responsável pela expedição do Edital e meio de contato:

Servidor responsável e resolução de designação: Thaís Spinola de Carvalho Varela, RDE.2025.147 de 08/08/2025
Endereço: Av. 4, nº 410, CAB, Salvador-BA. CEP:41.745-002

Horário: Segunda a quinta-feira das 08h30min às 12h e das 13h30min às 17h30min e às sextas-feiras das 08h30min às 12h e das 13h30min às 16h Tel: (71) 3115-7610 Email: licitacao@prodeb.ba.gov.br

20. Responsáveis pela elaboração e aprovação dos Estudos Técnicos Preliminares – ETP's, do Termo de Referência, da matriz de risco da contratação e do valor estimado referencial da licitação:

Nos termos da Cláusula Quinta, "k", do Termo de Cooperação Técnica nº 002/2026 celebrado entre o Estado da Bahia, por intermédio da Secretaria da Administração e a Companhia de Processamento de Dados do Estado da Bahia, a responsabilidade pela elaboração e validação dos instrumentos é da SAEB por intermédio da SGI, através do Superintendente, Sr. Thales José Costa de Almeida e da PRODEB, por intermédio da DTC, através do Diretor de Tecnologia e Conectividade, Sr. Carlos Augusto Borges Silva e do Assessor da DTC, Sr. Elmos Sales dos Santos.

Salvador - BA, 13 de maio de 2026.

PARTE I

SEÇÃO I

DOCUMENTOS QUE ACOMPANHAM A PROPOSTA DE PREÇOS REALINHADA APÓS A DISPUTA

O licitante deverá apresentar juntamente com a proposta de preços realinhada, na forma e prazo previstos na Parte III desde instrumento, sob pena de desclassificação, os seguintes documentos:

- (X) Descrição da proposta de preços;
- (X) Declaração de Enquadramento (apenas para as microempresas e empresas de pequeno porte que desejarem os benefícios da Lei Complementar nº 123/06 e suas alterações, preferencialmente de acordo com o modelo constante no ANEXO IV deste instrumento), nos termos do art. 1º, §3º do RLC da PRODEB e art. 4º, §2º da Lei Federal nº 14.133/2021.
- (X) Procuração, se for o caso, por instrumento público ou particular, este último acompanhado da prova da legitimidade de quem outorgou os poderes.
- (X) Outros documentos que devam acompanhar a proposta, definidos no item 13 no Termo de Referência.

SEÇÃO II ORÇAMENTO ESTIMADO EM PLANILHA

Nos termos do art. 46 do RLC da PRODEB e da justificativa apresentada ao item 19 do Termo de Referência, o orçamento estimado global do Lote 1 é de R\$ 589.983.785,00 (quinhentos e oitenta e nove milhões, novecentos e oitenta e três mil, setecentos e oitenta e cinco reais) e do Lote 2 é de R\$ 37.411.750,00 (trinta e sete milhões, quatrocentos e onze mil, setecentos e cinquenta reais), conforme previsto no Anexo III do Termo de Referência.

OBSERVAÇÃO: Conforme disposto no art. 83, IV do RLC da PRODEB, efetuado o julgamento dos lances ou propostas, será promovida a verificação de sua efetividade, promovendo-se a desclassificação daquelas que, além das demais hipóteses, se encontrem com valores unitários e global acima do orçamento estimado para a contratação, após esgotada a fase de lances e de negociação.

SEÇÃO III
MODELO DE DESCRIÇÃO DA PROPOSTA

1. MODELO DE DESCRIÇÃO DA PROPOSTA DE PREÇOS

Modalidade de Licitação	Número

Considerando as informações constantes no Edital, Termo de Referência e demais Anexos, segue modelo de proposta a ser apresentado:

LOTE 01							
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor mensal unitário (R\$) A	Valor unitário para 60 meses (R\$) B = A * 60	Valor Total 60 meses (R\$) C = B * QTD
1	02.81.00.00192352-8	Solução de Conectividade Segura TIPO 01 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 500MB.	Unidade	1589			

2	02.81.00.00192353-6	Solução de Conectividade Segura TIPO 02 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 2 links (redundância) de internet banda larga com velocidade de 500MB.	Unidade	707			
3	02.81.00.00192354-4	Solução de Conectividade Segura TIPO 03 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 1GB.	Unidade	109			
4	02.81.00.00192355-2	Solução de Conectividade Segura TIPO 04 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 2 links (redundância) de internet banda larga com velocidade de 1GB.	Unidade	167			

5	02.81.00.00192356-0	Solução de Conectividade Segura TIPO 05 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários em unidades remotas que não possuem viabilidade de conexão via fibra ótica, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 1 link satélite com velocidade de 100 MB.	Unidade	149			
6	02.81.00.00192357-9	Solução de Conectividade Segura TIPO 06 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 1 link de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.	Unidade	101			
7	02.81.00.00192358-7	Solução de Conectividade Segura TIPO 07 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 500MB.	Unidade	54			
8	02.81.00.00192359-5	Solução de Conectividade Segura TIPO 08 Solução de conectividade segura	Unidade	16			

		prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 500MB.					
9	02.81.00.00192360-9	Solução de Conectividade Segura TIPO 09 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 1GB.	Unidade	78			
10	02.81.00.00192361-7	Solução de Conectividade Segura TIPO 10 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 1GB.	Unidade	33			

11	02.81.00.00192362-5	Solução de Conectividade Segura TIPO 11 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB.	Unidade	91			
12	02.81.00.00192363-3	Solução de Conectividade Segura TIPO 12 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB e 1 link de internet banda larga com velocidade de 500MB.	Unidade	14			
13	02.81.00.00192364-1	Solução de Conectividade Segura TIPO 13 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades com até 40 usuários e que já possuem link de internet contemplando 01 firewall de próxima geração (NGFW) com tecnologia SD-WAN.	Unidade	105			

14	02.81.00.00192365-0	Solução de Conectividade Segura TIPO 14 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades acima de 40 usuários e que já possuem link de internet contemplando 01 firewall de próxima geração (NGFW) com tecnologia SD-WAN.	Unidade	50			
15	02.81.00.00192366-8	Solução de Conectividade Segura TIPO 15 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN, 2 links (redundância) de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.	Unidade	20			
16	02.81.00.00192367-6	Solução de Conectividade Segura TIPO 16 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN, 2 links (redundância) de internet banda larga com velocidade de 1GB e 1 link satélite com velocidade de 100 MB.	Unidade	16			

17	02.81.00.00192368-4	Solução de Conectividade Segura TIPO 17 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, destinada a unidades com até 05 usuários, contemplando 1 link de internet banda larga com velocidade de 200 Mbps e mecanismos de segurança providos de forma centralizada, sob gestão da PRODEB, sem a necessidade de firewall de borda dedicado na unidade.	Unidade	369		
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)
18	02.81.00.00192370-6	Serviço de Mudança de Endereço – até 300 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	137		
19	02.81.00.00192371-4	Serviço de Mudança de Endereço – acima de 300 km até 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	144		

20	02.81.00.00192372-2	Serviço de Mudança de Endereço – acima de 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	108			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor mensal unitário (R\$) A	Valor unitário para 60 meses (R\$) B = A * 60	Valor Total 60 meses (R\$) C = B * QTD
21	02.81.09.00008168-0	Solução de Operação e Monitoramento Central, prestada em regime contínuo e remunerada por valor mensal, dimensionada para atender até 500 (quinhentas) unidades de solução de conectividade segura em operação	Unidade	10			
22	02.81.09.00008169-8	Solução de Monitoramento e Relatoria De Logs Tipo I	Unidade	02			
23	02.81.00.00192944-5	Solução de Monitoramento e Relatoria De Logs Tipo II	Unidade	50			
24	02.81.00.00192945-3	Solução de Monitoramento e Relatoria De Logs Tipo III	Unidade	04			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)		Valor Total (R\$)
25	02.81.00.00192946-1	UST – Unidade de Serviços Técnicos	Unidade	5.000			
Valor Global do Lote 01:							

LOTE 02						
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)
1	02.81.00.00192373-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600E, pelo período de 12 meses	Unidade	04		
2	02.81.00.00192374-9	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 601E, pelo período de 12 meses	Unidade	04		
3	02.81.00.00192375-7	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 400F, pelo período de 12 meses	Unidade	08		
4	02.81.00.00192376-5	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200F, pelo período de 12 meses	Unidade	09		
5	02.81.00.00192377-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200E, pelo período de 12 meses	Unidade	04		

6	02.81.00.00192378-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 100F, pelo período de 12 meses	Unidade	24		
7	02.81.00.00192379-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 80F, pelo período de 12 meses	Unidade	12		
8	02.81.00.00192380-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 60F, pelo período de 12 meses	Unidade	300		
9	02.81.00.00192381-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 61F, pelo período de 12 meses	Unidade	300		
10	02.81.00.00192382-0	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 150G, pelo período de 12 meses	Unidade	04		
11	02.81.00.00192383-8	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 300G, pelo período de 12 meses	Unidade	04		

12	02.81.00.00192384-6	Serviço de Licenciamento e Atualização das Funcionalidades de Autenticação Centralizada de Usuários Marca Fortinet Modelo FortiAuthenticator 800F, pelo período de 12 meses	Unidade	04		
13	02.81.00.00192385-4	Solução De Segurança de Rede NGFW TIPO I, com licenciamento pelo período de 12 meses	Unidade	04		
14	02.81.00.00192386-2	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede - Segmentação Interna TIPO I, pelo período de 12 meses	Unidade	04		
15	02.81.00.00192947-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3700F, pelo período de 12 meses	Unidade	04		
16	02.81.00.00192948-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3301E, pelo período de 12 meses	Unidade	04		
17	02.81.00.00192949-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3000D, pelo período de 12 meses	Unidade	02		

18	02.81.00.00192950-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600F, pelo período de 12 meses	Unidade	04		
19	02.81.00.00192951-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 40F, pelo período de 12 meses	Unidade	60		
20	02.81.00.00192952-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate-VM08, pelo período de 12 meses	Unidade	02		
21	02.81.00.00192953-4	Serviço de Licenciamento e Atualização das Funcionalidades de WAF Marca Fortinet Modelo FortiWeb2000F, pelo período de 12 meses	Unidade	04		
22	02.81.00.00192954-2	Serviço de Licenciamento e Atualização das Funcionalidades de ADC Marca Fortinet Modelo FortiADC-400F, pelo período de 12 meses	Unidade	02		
23	02.80.00.00192955-0	Serviço de Licenciamento e Atualização das Funcionalidades de Gerenciador Centralizada de Dispositivos Marca Fortinet Modelo FortiManager 3000G, pelo período de 12 meses	Unidade	02		

24	02.81.00.00192956-9	Serviço de Licenciamento e Atualização das Funcionalidades de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	02		
25	02.81.00.00192957-7	Serviço de Upgrade para 50 Devices e 500 EPS de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	04		
26	02.81.00.00192958-5	Solução De Segurança de Aplicações WAF - TIPO I, com licenciamento pelo período de 12 meses	Unidade	02		
27	02.81.00.00192959-3	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF - TIPO I, pelo período de 12 meses	Unidade	02		
28	02.81.00.00192989-5	Solução De Segurança de Aplicações WAF - TIPO II, com licenciamento pelo período de 12 meses	Unidade	10		
29	02.81.00.00192990-9	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF –TIPO II, pelo período de 12 meses	Unidade	10		
30	02.81.00.00192962-3	Solução de Segurança de Aplicações WAF para Ambientes Híbridos, com licenciamento pelo período de 12 meses	Unidade	10		
31	02.81.00.00192963-1	Serviço de Licenciamento e Atualização das Funcionalidades de Solução de Segurança de Aplicações WAF para Ambientes Híbridos, pelo período de 12 meses	Unidade	10		
32	02.81.00.00192964-0	Solução de Segurança Decoy/Honeypot, com licenciamento pelo período de 12 meses	Unidade	06		

33	02.81.00.00192965-8	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança Decoy/Honeypot, pelo período de 12 meses	Unidade	06		
34	02.81.00.00192966-6	Solução de Segurança de Rede NGFW TIPO II, com licenciamento pelo período de 12 meses	Unidade	100		
35	02.81.00.00192967-4	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna TIPO II, pelo período de 12 meses	Unidade	100		
36	02.81.00.00192968-2	Solução de Segurança de Rede NGFW TIPO III, com licenciamento pelo período de 12 meses	Unidade	50		
37	02.81.00.00192969-0	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna TIPO III, pelo período de 12 meses	Unidade	50		
Valor Global do Lote 02						R\$

Salvador ____ de _____ de 20__.

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

OBSERVAÇÃO 1: NÃO SERÃO ACEITAS PROPOSTAS COM VALORES UNITÁRIO E GLOBAL SUPERIORES AO ESTIMADO.

OBSERVAÇÃO 2: A proposta de preços deverá ser acompanhada por todos os documentos listados no Parte I, Seção I deste Edital, bem como deve atender ao item 13 do Termo de Referência, **sob pena de desclassificação.**

PARTE II
HABILITAÇÃO E CONDIÇÕES PARA CONTRATAÇÃO

1. Para a habilitação dos interessados, exigir-se-ão os documentos relativos a:

1.1 Habilitação jurídica, comprovada mediante a apresentação:

(X) Para pessoas jurídicas:

- a) empresário individual: inscrição no registro público de empresas mercantis;
- b) microempreendedor individual – MEI: certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;
- c) sociedade empresária, sociedade limitada unipessoal: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, com suas eventuais alterações supervenientes em vigor, devidamente registrados, acompanhados, quando for o caso, dos documentos societários comprobatórios de eleição ou designação e investidura dos atuais administradores.
- d) sociedades simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, com suas eventuais alterações supervenientes em vigor, devidamente registrados, acompanhados dos atos comprobatórios de eleição e investidura dos atuais administradores.
- e) empresa ou sociedade estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, observando-se a Instrução Normativa DREI/ME nº 77, de 18 de março de 2020, quando a atividade assim o exigir.
- f) filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz.
- g) prova de inscrição no Cadastro Nacional de Pessoa Jurídica – CNPJ;
- h) prova de inscrição no Cadastro de Contribuinte Estadual ou Municipal, se houver, relativo ao domicílio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- i) declaração unificada, conforme modelo constante no Anexo V deste Edital.

NOTA 01: Conforme previsto no art. 92, § 1º do RLC da PRODEB, a documentação requerida relativa à habilitação jurídica (exceto alíneas “g”, “h” e “i”) pode ser substituída pela Certidão Simplificada expedida pela Junta Comercial, para firmas individuais (Empresário) ou sociedades mercantis (Sociedade Empresária), ou Certidão em breve relatório expedida pelo Registro Civil das Pessoas Jurídicas para as Sociedades Cívis.

NOTA 02: Conforme art. 92, § 2º do RLC da PRODEB, o objeto social especificado nos documentos acima determina a participação da Empresa nas licitações promovidas pela PRODEB, devendo ser totalmente compatível com o objeto licitado.

1.2 Qualificação Técnica – Item 14 do TR:

- a) Para fins de habilitação técnica, a licitante arrematante deve apresentar, na forma e nos prazos indicados no edital, documentos de comprovação quanto à capacidade técnico-operacional.
- b) Os documentos devem ser apresentados em língua portuguesa, com a ressalva que serão aceitos documentos técnicos, e datasheets em língua inglesa devido à ausência de tradução das Terminologias Técnicas.
- c) **LOTE 1:** A PROPONENTE deverá apresentar atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, comprovando que prestou serviços de Solução de conectividade segura, incluindo proteção de borda, firewall de próxima geração (NGFW) com tecnologia SD-WAN, links de internet e Solução de Operação e Monitoramento Central, incluindo instalação, configuração e suporte. É exigido que seja apresentado um ou mais atestados, cuja soma totalize pelo menos 20% (vinte por cento) do quantitativo total estimado.
 - c.1) A exigência de apresentação de atestado(s) de capacidade técnica prevista no item 14.4 justifica-se pela complexidade técnica, criticidade operacional e abrangência territorial da solução de conectividade segura, que envolve a prestação integrada de serviços de rede e segurança gerenciados a elevado número de unidades distribuídas geograficamente. Assim, mostra-se necessária a comprovação da capacidade técnico-operacional da licitante por meio de experiência prévia na execução de serviços semelhantes ou compatíveis em características e quantidades com o objeto da contratação, em escala suficiente para mitigar riscos de inexecução contratual, admitindo-se a apresentação de um ou mais atestados que evidenciem tal aptidão, nos termos definidos neste Termo de Referência.
- d) **LOTE 2:** A PROPONENTE deverá apresentar atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, comprovando que prestou serviços solução de segurança da informação e cibersegurança, compreendendo licenciamento, atualização e garantia. É exigido que seja apresentado um ou mais atestados, cuja soma totalize pelo menos 20% (vinte por cento) do quantitativo total estimado.
 - d.1) O percentual de 20% (vinte por cento) se justifica para comprovar a capacidade técnico-operacional da licitante para o desempenho de atividade pertinente e compatível em características e quantidades com o objeto da licitação, mitigando assim, os riscos de inexecução do contrato.

LOTE	Descritivo dos Itens	QTD Total (100%)	Comprovaçã o (20%)
LOTE 01	Solução de Conectividade Segura com NGFW e Link de Internet - Incluindo instalação, configuração, sustentação e suporte técnico durante a vigência contratual, com características técnicas semelhantes às especificadas neste Termo de Referência	4571	914

LOTE 02	Solução De Segurança de Aplicações WAF	12	02
	Solução De Segurança de Rede Ambiente Híbridos	10	02
	Solução De Segurança de Rede Segmentação Interna	154	30

- e) Todas as informações citadas acima deverão constar de forma explícita no(s) atestado(s).
- f) A proposta da licitante deverá vir acompanhada de documentação técnica que comprove o atendimento dos requisitos, incluindo os datasheets dos equipamentos.
- g) É preferível que os atestados emitidos por pessoa jurídica de direito privado contenham assinatura digital certificada ou com reconhecimento de firma, que assegure sua autenticidade. Caso a assinatura do responsável técnico não contenha elemento de autenticação, a Prodeb se resguarda ao direito de realizar diligência para solicitar documentos a fim de sanar eventuais dúvidas quanto ao referido atestado.
- h) A CONTRATANTE se reserva o direito de conferir as informações prestadas pelas empresas emitentes dos atestados, através de consultas e visitas, bem como a disponibilidade de equipamentos solicitados junto à PROPONENTE.
- i) A LICITANTE deverá apresentar relação explícita e declaração formal de disponibilidade dos recursos humanos e materiais necessários, sob as penas da lei, especialmente o disposto no art. 155, inc. VIII, da Lei nº 14.133/2021 e art. 211 do RLC da Prodeb.
- j) Deverá ser apresentado profissionais técnicos pertencentes ao quadro da empresa — sócios, empregados ou prestadores de serviços — devidamente capacitados pelo fabricante para realizar a instalação, configuração e manutenção dos itens ofertados, com comprovação por certificados de qualificação vigentes emitidos pelo fabricante, conforme quantitativos abaixo:

LOTE	Descrição da Certificação	QTD Total
LOTE 01	Certificação de Solução de Gestão e Relatoria de Logs	01
	Certificação de NGFW e ou SDWAN para Solução de Conectividade Segura.	10
	Certificação de Plataforma Centralizada de Gerenciamento de Dispositivos.	01
	Certificação de Solução de Zero Trust Access.	02
	Certificação em ITIL Foundation Certificate in IT Service Management	01
	Diploma de Pós-graduação e ou MBA em Gestão de Projetos	02
LOTE 02	Certificação de Solução De Segurança de Aplicações WAF.	01
	Certificação de Solução de Rede NGFW	03

- k) Além das certificações descritas na tabela acima, a licitante deverá comprovar que ao menos 01 (um) profissional possui registro profissional ativo no respectivo conselho competente (CREA ou CFT), compatível com as atribuições técnicas inerentes ao objeto contratado.
- l) A relação dos profissionais técnicos deverá estar acompanhada de comprovação de vínculo com a licitante, mediante a apresentação de, no mínimo, um dos seguintes documentos, conforme o caso:
 - l.1) CTPS;
 - l.2) Contrato social;
 - l.3) Contrato de prestação de serviços;
 - l.4) Termo de compromisso de integração ao quadro técnico no caso de adjudicação.
- m) Os profissionais indicados deverão participar efetivamente da execução contratual, sendo admitida substituição apenas por profissionais de experiência equivalente ou superior, com anuência da Administração.

1.3 Qualificação econômico-financeira – Item 15 do TR:

A ser comprovada mediante:

- a) A licitante deverá apresentar certidão negativa de falência expedida pelo distribuidor da sede do licitante, com data de expedição ou revalidação dos últimos 90 (noventa) dias anteriores à data da realização da licitação, caso o documento não consigne prazo de validade;
- b) A licitante deverá apresentar índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

$$\text{Liquidez Geral (LG)} = (\text{Ativo Circulante} + \text{Realizável a Longo Prazo}) / (\text{Passivo Circulante} + \text{Passivo Não Circulante});$$

$$\text{Solvência Geral (SG)} = \text{Ativo Total} / (\text{Passivo Circulante} + \text{Passivo Não Circulante});$$

$$\text{Liquidez Corrente (LC)} = \text{Ativo Circulante} / \text{Passivo Circulante}.$$

b.1) Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) ou Liquidez Corrente (LC), será exigido, para fins de habilitação econômico-financeira, patrimônio líquido mínimo correspondente a 10% (dez por cento) do valor estimado da contratação, devendo a comprovação observar, como base de cálculo, o valor estimado fixado pela PRODEB, e não o valor final da proposta apresentada pelo licitante.

b.2) O balanço patrimonial, a demonstração do resultado do exercício e as demais demonstrações contábeis limitar-se-ão ao último exercício, caso a pessoa jurídica tenha sido constituída há menos de 2 (dois) anos, nos termos do art. 69, §6º, da Lei Federal nº 14.133/2021.

b.3) O balanço patrimonial e as demonstrações contábeis poderão ser atualizados por índices oficiais quando encerrados há mais de 3 (três) meses da data da apresentação da proposta, vedada a sua substituição por balancetes ou balanços provisórios.

b.4) O licitante apresentará o balanço patrimonial e a demonstração do resultado do exercício mediante, conforme o caso, publicação em Diário Oficial ou jornal de grande circulação, registro na Central de Balanços no âmbito do Sistema Público de Escrituração Digital – SPED, ou cópia reprográfica das páginas do Livro Diário, com os respectivos Termos de Abertura e Encerramento registrados na Junta Comercial.

b.5) O atendimento dos índices econômicos previstos neste subitem será atestado mediante declaração assinada por profissional legalmente habilitado da área contábil, apresentada pelo licitante, nos termos do art. 69, §1º, da Lei Federal nº 14.133/2021.

b.6) Na hipótese de participação de empresas reunidas em consórcio, conforme previsto para o Lote 1, conforme previsto para o Lote 01, a verificação dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC) será realizada com base nos valores consolidados, obtidos pela soma dos ativos e passivos correspondentes das empresas consorciadas, vedada a simples soma ou média dos índices individuais.

b.6.1) A título exemplificativo, considerando um consórcio composto por duas empresas, sendo a Empresa A com Ativo Circulante de R\$ 20.000.000,00 (vinte milhões de reais), Realizável a Longo Prazo de R\$ 10.000.000,00 (dez milhões de reais), Passivo Circulante de R\$ 15.000.000,00 (quinze milhões de reais) e Passivo Não Circulante de R\$ 5.000.000,00 (cinco milhões de reais), e a Empresa B com Ativo Circulante de R\$ 30.000.000,00 (trinta milhões de reais), Realizável a Longo Prazo de R\$ 20.000.000,00 (vinte milhões de reais), Passivo Circulante de R\$ 25.000.000,00 (vinte e cinco milhões de reais) e Passivo Não Circulante de R\$ 10.000.000,00 (dez milhões de reais), o cálculo do Índice de Liquidez Geral (LG) deverá considerar os valores consolidados do consórcio. Nesse caso, o Ativo Circulante consolidado será de R\$ 50.000.000,00 (cinquenta milhões de reais), o Realizável a Longo Prazo consolidado de R\$ 30.000.000,00 (trinta milhões de reais), o Passivo Circulante consolidado de R\$ 40.000.000,00 (quarenta milhões de reais) e o Passivo Não Circulante consolidado de R\$ 15.000.000,00 (quinze milhões de reais), resultando em Índice de Liquidez Geral (LG) igual a 1,45, obtido pela aplicação da fórmula prevista no item "b".

b.7) Na hipótese de participação de empresas reunidas em consórcio, caso o resultado apurado de forma consolidada seja inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) ou Liquidez Corrente (LC), será exigido, para fins de habilitação econômico-financeira, o patrimônio líquido mínimo correspondente ao percentual previsto no item 16.1, observado que, quando o consórcio não for formado integral ou exclusivamente por microempresas ou empresas de pequeno porte, o referido percentual será acrescido de 10% (dez por cento) em relação ao exigido para os licitantes individuais.

b.7.1) A título exemplificativo, considerando uma contratação cujo valor estimado seja de R\$ 100.000.000,00 (cem milhões de reais), o patrimônio líquido mínimo exigido nos termos do item "b.1" corresponderá a R\$ 10.000.000,00 (dez milhões de reais). Na hipótese de participação de consórcio não formado integral ou exclusivamente por microempresas ou empresas de pequeno porte, e verificada a necessidade de comprovação de patrimônio líquido mínimo nos termos do item "b.7", o valor exigido será acrescido de 10% (dez por cento), totalizando R\$ 11.000.000,00 (onze milhões de reais), podendo tal montante ser comprovado de forma consolidada pela soma dos patrimônios líquidos das empresas consorciadas.

1.4 Habilitação fiscal, social e trabalhista

a) prova de regularidade com a Fazenda (X) Estadual/Distrital (X) Municipal/Distrital do domicílio ou sede do prestador de serviço, relativa à atividade em cujo exercício contrata ou concorre;

a.1) Caso o licitante seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

b) prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social.

c) prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

d) prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

e) em se tratando de contratação direta, prova de regularidade com a Fazenda do Estado da Bahia, ou o compromisso de sua regularização e sua efetiva realização, como condição para celebração do contrato, nos termos do art. 65 da Lei estadual nº 14.634, de 2023.

1.4.1 As microempresas e empresas de pequeno porte, beneficiárias do tratamento diferenciado e favorecido previsto na Lei Complementar nº 123/06, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição.

1.5 Declaração de Proteção ao Trabalho do Menor

Conforme o inciso XXXIII do art. 7º da Constituição Federal, para os fins do disposto no art. 45, §2º, I, "e" do RLC da PRODEB, deverá declarar quanto ao trabalho do menor, conforme consta na Declaração Unificada do **ANEXO V** deste instrumento.

2. Regras acerca da participação de matriz e filial

- a) Se a licitante for a matriz, todos os documentos devem estar em nome da matriz;
- b) Se a licitante for filial, todos os documentos devem estar em nome da filial, exceto aqueles que a legislação permita ou exija a emissão apenas em nome da matriz;
- c) A comprovação de capacidade operacional para o desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação poderá ser feita em nome da matriz ou da filial;
- d) Se a licitante participar do certame apresentando os documentos de habilitação e qualificação da matriz e desejar executar o contrato pela filial, ou vice-versa, deverá fazer prova, por ocasião da assinatura do contrato, da regularidade do estabelecimento que executará o objeto licitado, a qual deverá ser mantida durante todo o curso da avença.

3. A licitante deverá apresentar/enviar os documentos acima relacionados, sob pena de inabilitação, sendo-lhe facultado apresentar, alternativamente, o Certificado de Registro Cadastral-CRC ou Certificado de Registro Simplificado-CRS ou Registro de Cadastro de Fornecedores - SICAF, que possibilitará a substituição dos documentos de habilitação, exceto os concernentes à Qualificação Técnica, conforme estabelecido no art. 100, §2º do RLC da PRODEB e na forma indicada neste instrumento.

3.1 Caso conste do registro algum documento vencido, a licitante deverá apresentar/enviar a versão atualizada do referido documento.

3.2 No pregão eletrônico, os documentos de habilitação deverão ser apresentados conforme o disposto na Parte III do presente instrumento.

4. A licitante vencedora deve observar as condições estabelecidas para o momento da contratação, previstas no item 31.2 do Termo de Referência e na Parte III deste Instrumento.

5. A contratada deverá cumprir o quanto estabelecido no item 23 (Proteção de Dados Pessoais), no item 28 (exigência do Programa de Integridade – Lote 1) e no item 29 (Requisitos de Sustentabilidade e Acessibilidade – Lotes 1 e 2) do Termo de Referência.

PARTE III

SEÇÃO I - RITO PROCEDIMENTAL

1. DIRETRIZES

1.1 O rito procedimental da presente licitação seguirá o disposto nesta Seção, relativamente à operacionalização das fases do procedimento da licitação pelo critério de julgamento adotado, na forma eletrônica.

1.1.1 Para fins deste Edital, considera-se responsável pela licitação o agente de contratação ou comissão de contratação a quem compete a condução do procedimento licitatório.

1.1.2 No caso da modalidade pregão, aplicável ao critério de julgamento por menor preço o maior desconto, o agente de contratação será designado pregoeiro.

1.2 Na presente licitação será observado o que se segue:

- a) os documentos serão produzidos por escrito, com data e local de sua realização e assinatura dos responsáveis;
- b) os valores, os preços e os custos utilizados terão como expressão monetária a moeda corrente nacional; e
- c) o desatendimento de exigências meramente formais que não comprometam a aferição da qualificação dos licitantes ou a compreensão do conteúdo de suas propostas não importará seu afastamento da licitação ou a invalidação do processo;
- d) será disponibilizado o acesso aos documentos que compõem as propostas e os documentos de habilitação apresentados no processo licitatório.

2. ORDEM DAS FASES DA LICITAÇÃO

2.1 A realização da licitação observará as seguintes fases sucessivas:

2.1.1. Quando adotado o critério menor preço ou maior desconto:

a) preparatória; b) divulgação do edital de licitação; c) apresentação de propostas e lances; d) julgamento; e) habilitação; f) recurso; e g) homologação.

2.1.2. Quando adotado o critério técnica e preço:

a) preparatória; b) divulgação do edital de licitação; c) apresentação de propostas técnica e de preço; d) julgamento; e) habilitação; f) recurso; e g) homologação.

2.2 Na hipótese de inversão de fases, desde que observados os requisitos do art. 17, §1º, da Lei Federal nº 14.133/2021 e art. 42, § único do RLC/PRODEB, e que seja disponibilizada a funcionalidade no sistema eletrônico, a fase de habilitação antecederá as fases de apresentação de propostas.

3. PARTICIPAÇÃO NA LICITAÇÃO

3.1 O *site*, dia e hora para recebimento das propostas e início da sessão pública estão indicados no Preâmbulo deste Edital.

3.1.1 Reputa-se credenciada a pessoa natural regularmente designada para representar a licitante no processo licitatório.

3.1.2 Cada licitante poderá credenciar apenas um representante e cada representante somente poderá representar uma única licitante.

3.2 O licitante deverá credenciar-se previamente no sistema eletrônico utilizado no certame.

3.2.1 O credenciamento do usuário implica em sua responsabilidade legal e na presunção de capacidade técnica para realização das transações inerentes à licitação.

3.2.2 O credenciamento do usuário será pessoal e intransferível para acesso ao sistema, sendo o licitante responsável por todos os atos praticados.

3.3 O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, quando houver, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou da PRODEB por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

3.4 Não poderão disputar esta licitação:

- a) aquele que não atenda às condições deste Edital e seu(s) anexo(s);
- b) autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre obra, serviços ou fornecimento de bens a ele relacionados;
- c) empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre obra, serviços ou fornecimento de bens a ela necessários;
- d) pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

- e) aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente da contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;
- f) empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;
- g) pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação deste edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;
- h) agente público do órgão ou entidade licitante;
- i) Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;
- 3.4.1 Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria.
- 3.5 O impedimento relativo a pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta, será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.
- 3.6 A critério da PRODEB e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem as alíneas "b" e "c" do subitem 3.4 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.
- 3.7 Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.
- 3.8 O disposto nas alíneas "b" e "c" do subitem 3.4 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.
- 3.9 Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea.
- 3.10 As vedações de que tratam a alínea "h" do subitem 3.4 e o subitem 3.4.1 se estendem a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

Tratamento diferenciado e simplificado (Lei Complementar nº 123/2006, art. 4º da Lei Federal nº 14.133/2021 e arts. 89 e 90 do RLC/PRODEB)

3.11 Na concessão do tratamento diferenciado e simplificado, deverão ser observadas as disposições constantes dos arts. 42 a 49 da Lei Complementar nº 123, de 14 de dezembro de 2006, observado o disposto no art. 4º da Lei Federal nº 14.133/2021 e arts. 89 e 90 do RLC/PRODEB.

Aquisição com reserva de cotas (não se aplica)

- 3.12 No caso de aquisição com reserva de cotas, serão observadas as seguintes disposições:
- 3.12.1 O percentual da cota reservada do quantitativo licitado está definido no TR/HABILITAÇÃO, a qual será destinada às microempresas e empresas de pequeno porte, nos termos do art. 48, inc. III, da Lei Complementar nº 123/06.
- 3.12.2 A cota será disputada em lote apartado, do qual participarão apenas as microempresas e empresas de pequeno porte.
- 3.12.3 A reserva da cota não impede a contratação das microempresas ou das empresas de pequeno porte na totalidade do objeto.
- 3.12.4 Na hipótese de não haver vencedor para a cota reservada, esta poderá ser adjudicada ao vencedor da cota principal ou, diante de sua recusa, aos licitantes remanescentes, desde que pratiquem o preço do primeiro colocado da cota principal.
- 3.12.5 Se a mesma empresa vencer a cota reservada e a cota principal, a contratação das cotas deverá ocorrer pelo menor preço.
- 3.12.6 Deverá ser priorizada a aquisição dos produtos das cotas reservadas, ressalvados os casos em que a cota reservada seja inadequada para atender as quantidades ou as condições do pedido, justificadamente.

4. DO CADASTRAMENTO DA PROPOSTA INICIAL

Disposições gerais

4.1. Os licitantes cadastrarão, exclusivamente por meio do sistema eletrônico, as suas propostas, até a data e o horário estabelecidos para abertura da sessão pública no Preâmbulo do Edital.

4.2 Na hipótese de inversão de fases, os licitantes encaminharão os documentos de habilitação simultaneamente com o cadastramento das propostas, na forma e no prazo estabelecidos no subitem 4.1.

4.3 No cadastramento das propostas, o licitante declarará, em campo próprio do sistema eletrônico:

- a) a inexistência de fato impeditivo para licitar ou contratar com a Administração Pública;
- b) o pleno conhecimento e aceitação das regras e das condições gerais da contratação, constantes deste Edital;
- c) a responsabilidade pelas transações que forem efetuadas no sistema eletrônico, assumindo-as como firmes e verdadeiras;
- d) o cumprimento do disposto no inc. VI do art. 68 da Lei Federal nº 14.133/2021 e art. 91, V do RLC/PRODEB;
- e) o cumprimento dos requisitos para habilitação e a conformidade de suas propostas com as exigências deste Edital.

4.3.1 Ao cumprir o disposto nas alíneas "b" e "e" do subitem 4.3, o licitante automaticamente declara:

- a) a aceitação de todas as condições dos anexos deste Edital;
- b) que a proposta de preços apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo, nos termos do §1º do art. 63 da Lei Federal nº 14.133/2021;
- c) não possuir empregados executando trabalho degradante ou forçado, observando o disposto nos incs. III e IV do art. 1º e no inc. III do art. 5º da Constituição Federal;
- d) que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, nos termos do inc. IV do art. 63 da Lei Federal nº 14.133/2021.

4.3.2 A declaração firmada em campo próprio do sistema eletrônico será suficiente para fazer prova da exigência nele contida, ressalvada a possibilidade de realização de diligência pelo responsável pela licitação para esclarecimentos adicionais, caso necessário.

4.3.2.1 O não atendimento, pelo licitante, de diligência a ele dirigida, será reputado desistência, implicando na sua exclusão do certame, sem prejuízo das consequências definidas na legislação.

4.3.2.2 A declaração que for comprovada falsa implicará na exclusão do licitante, sem prejuízo de apuração de responsabilidade.

4.4 O licitante enquadrado como microempresa ou empresa de pequeno porte deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no art. 3º da Lei Complementar nº 123/2006, estando apto a usufruir do tratamento estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º da Lei Federal nº 14.133/2021 e art. 45, §2º, I do RLC/PRODEB.

4.5 A falsidade de qualquer declaração de que trata o item 4 sujeitará o licitante às sanções previstas neste Edital, na Lei Federal nº 14.133/2021, as referidas na Lei nº 14.634/2023 e no RLC/PRODEB.

4.6 Os licitantes poderão retirar ou substituir as propostas e, quando for o caso, os documentos de habilitação, anteriormente inseridos no sistema, até a abertura da sessão pública.

4.7. Na hipótese de inversão de fases, os licitantes poderão retirar ou substituir os documentos de habilitação anteriormente inseridos no sistema eletrônico, até a abertura da sessão pública.

4.8 Não haverá ordem de classificação na etapa de apresentação das propostas e dos documentos de habilitação pelo licitante.

Acompanhamento do sistema

4.9 Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela PRODEB ou de sua desconexão.

Parametrização do valor ou do percentual de desconto

4.10 Quando adotado o critério menor preço ou maior desconto, serão observadas as disposições dos subitens seguintes.

4.10.1 Desde que disponibilizada a funcionalidade no sistema eletrônico, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá as seguintes regras:

- a) a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e
- b) os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata a alínea "a" deste subitem.

4.10.2 Desde que disponibilizada a funcionalidade no sistema eletrônico, o valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo licitante durante a fase de disputa, sendo vedado:

- a) valor superior a lance já registrado pelo licitante no sistema, quando adotado o critério de julgamento por menor preço; e
- b) percentual de desconto inferior a lance já registrado pelo licitante no sistema, quando adotado o critério de julgamento por maior desconto.

4.10.3 O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do subitem 4.10.1 possuirá caráter sigiloso para os demais licitantes e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

5. DO CONTEÚDO DA PROPOSTA

5.1 O licitante deverá elaborar a sua proposta em conformidade com o que dispõe o TR/Habilitação.

5.2 Todas as especificações do objeto contidas nas propostas vinculam o licitante.

5.3 Nos valores resultantes da proposta estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

5.3.1 Estarão contemplados ainda todos os custos com material de consumo, fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, tributos, impostos, taxas, emolumentos e quaisquer outros custos que, se relacionem com o fiel cumprimento pelo licitante das obrigações,

5.3.2 A eventual exceção à previsão deste subitem deverá constar expressamente do TR/Habilitação.

5.4 A proposta ofertada pelo licitante é de sua exclusiva responsabilidade, inclusive no que respeita ao percentual de desconto, preço ou lance, quando for o caso, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

5.5 Com a apresentação das propostas, o proponente assume o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

5.5.1 Os licitantes devem respeitar os preços máximos fixados pela PRODEB ou por órgão oficial competente ou constantes de tabela de preços referenciais.

5.5.2 Caso o critério de julgamento seja o de maior desconto, o preço resultante da aplicação do desconto ofertado deverá respeitar os preços máximos fixados pela PRODEB ou por órgão oficial competente ou constantes da tabela de preços referenciais.

5.6 Somente será admitida a indicação da tributação relativa ao Simples Nacional pelos licitantes que explorem as atividades de serviço de vigilância, limpeza ou conservação, de forma exclusiva ou em conjunto com outras atividades que não tenham sido objeto de vedação à inclusão no Simples, conforme previsto no art. 17, §1º, c/c art. 18, §5º-C, inc. VI, da Lei Complementar nº 123/2006, devendo observar, ainda, no que respeita ao serviço de vigilância, o disposto na Lei Federal nº 14.967, de 9 de setembro de 2024.

5.7 Nas licitações destinadas à contratação de serviços com fornecimento de mão de obra em regime de dedicação exclusiva que não sejam de serviço de vigilância, limpeza ou conservação, o licitante incluído no Simples Nacional deverá formular proposta considerando a tributação comum aplicável aos serviços, sob pena de desclassificação.

5.7.1 Na hipótese do subitem 5.7, o licitante que venha a ser contratado estará sujeito à exclusão obrigatória do Simples Nacional a contar do mês seguinte ao da contratação, em face do disposto no art. 31, inc. II, da Lei Complementar nº 123/2006.

5.7.2 O pedido da exclusão do Simples Nacional deverá ser feito no prazo previsto no art. 30, §1º, inc. II, da Lei Complementar nº 123/2006, devendo a contratada apresentar cópia do ofício encaminhado à Receita Federal do Brasil, com comprovante de recebimento, como condição para recebimento da primeira fatura da prestação dos serviços.

6. ABERTURA DA SESSÃO PÚBLICA

6.1 A abertura da licitação se dará automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados no Preâmbulo deste Edital.

6.1.1 Havendo necessidade de suspensão da sessão pública, o responsável pela licitação informará a data e horário previsto para a reabertura da sessão.

7. ETAPA ANTECEDENTE AO JULGAMENTO

7.1 CONTEÚDO APLICÁVEL EXCLUSIVAMENTE AO CRITÉRIO MENOR PREÇO E MAIOR DESCONTO

Lances

7.1.1 Na fase competitiva será observado o que se segue:

7.1.1.1 Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico.

7.1.1.2 Ressalvada a hipótese de parametrização referida no subitem 4.9, é vedado ao licitante apresentar seus lances de forma sucessiva, padronizada, intermitente, simultânea ou em intervalos de poucos segundos entre eles, ou de outros mecanismos indicativos da utilização de software lançador "robô".

7.1.1.3 Se inobservada a vedação estabelecida no subitem 7.1.1.2, o responsável pela licitação desclassificará a proposta e determinará a consequente abertura de processo administrativo para apuração do ilícito.

7.1.1.4 Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas neste Edital.

7.1.1.5 O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior, conforme o caso, ao último por ele ofertado e registrado pelo sistema.

7.1.1.6 Será aplicado intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta (degrau).

7.1.1.6.1 O degrau deverá ser aquele indicado no TR/Habilitação.

7.1.1.7 Caso o sistema eletrônico disponibilize essa funcionalidade, o licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de 15 (quinze) segundos após o registro no sistema eletrônico, na hipótese de lance inconsistente ou inexequível.

7.1.1.8 Não serão aceitos 2 (dois) ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

7.1.1.9 Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

7.1.1.10 Na hipótese de o sistema eletrônico se desconectar no decorrer da etapa de envio de lances da sessão pública e permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

7.1.1.11 Caso, durante a desconexão do sistema eletrônico para o responsável pela licitação, ocorra o encerramento da disputa, o responsável pela licitação dará prosseguimento aos atos do certame somente após decorridas 24 (vinte e quatro) horas da comunicação do fato aos participantes, no sítio eletrônico utilizado para divulgação deste Edital.

7.1.1.12 Caso não sejam apresentados lances pelos licitantes, o julgamento será feito com a proposta inicial.

Fluxo do procedimento segundo o modo de disputa

7.1.2 O procedimento seguirá de acordo com o modo de disputa adotado.

7.1.2.1 No **modo de disputa "aberto"**, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

7.1.2.1.1 A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

7.1.2.1.2 A prorrogação automática da etapa de lances de que trata o subitem 7.1.2.1.1 será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

7.1.2.1.3 Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública será encerrada automaticamente e o sistema ordenará e divulgará os lances, segundo a ordem crescente de valores ou decrescente de percentual de desconto, conforme o critério de julgamento adotado.

7.1.2.1.4 Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o responsável pela licitação poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

7.1.2.1.5 Após o reinício previsto no subitem 7.1.2.1.4, os licitantes serão convocados para apresentar lances intermediários.

7.1.2.2 No **modo de disputa "aberto e fechado"** os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

7.1.2.2.1 A etapa de lances da sessão pública terá duração inicial de 15 (quinze) minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até 10 (dez) minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

7.1.2.2.2 Encerrado o prazo previsto no subitem 7.1.2.2.1, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo ou de maior percentual de desconto, conforme o critério de julgamento adotado, e os das ofertas com preços até 10% (dez por cento) superiores ou inferiores àquela possam ofertar um lance final e fechado em até 5 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

7.1.2.2.3 No procedimento de que trata o subitem 7.1.2.2.2, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

7.1.2.2.4 Não havendo pelo menos 3 (três) ofertas nas condições definidas neste subitem, o sistema possibilitará aos autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de 3 (três), oferecer um lance final e fechado em até 5 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

7.1.2.2.5 Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores ou decrescente de percentual de desconto, conforme o critério de julgamento adotado.

7.1.2.3 No **modo de disputa "fechado e aberto"** somente serão classificados para a etapa da disputa aberta, com a apresentação de lances públicos e sucessivos, o licitante que apresentou a proposta de menor preço ou de maior percentual de desconto e os das propostas até 10% (dez por cento) superiores ou inferiores àquela, conforme o critério de julgamento adotado.

7.1.2.3.1 Não havendo pelo menos 3 (três) propostas nas condições definidas no subitem 7.1.2.3 **Erro! Fonte de referência não encontrada.**, poderão os licitantes que apresentaram as 3 (três) melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

7.1.2.3.2 A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

7.1.2.3.3 A prorrogação automática da etapa de lances de que trata o subitem 7.1.2.3.2 será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

7.1.2.3.4 Não havendo novos lances na forma estabelecida nos subitens anteriores, a sessão pública será encerrada automaticamente, e o sistema ordenará e divulgará os lances, segundo a ordem crescente de valores ou decrescente de percentual de desconto, conforme o critério de julgamento adotado.

7.1.2.3.5 Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o responsável pela licitação poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

7.1.2.3.6 Após o reinício previsto no subitem 7.1.2.3.5, os licitantes serão convocados para apresentar lances intermediários, podendo optar por manter o seu último lance.

Situações de empate

7.1.3 Em caso de empate, será observado o que se segue:

7.1.3.1 Ocorrendo **empate real**, será observado o procedimento a seguir definido.

7.1.3.1.1 Só poderá haver empate entre propostas iguais (não seguidas de lances) ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.1.3.1.2 Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 90 do RLC/PRODEB e no art. 60 da Lei Federal nº 14.133/2021, nesta ordem:

a) disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

b) avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos na Lei Federal nº 14.133/2021;

c) desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme o art. 4º, §§1º a 3º, do Decreto nº 22.665/2024;

d) desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

7.1.3.1.2.1 A comprovação do desenvolvimento de ações de equidade e de programa de integridade a que se referem as alíneas "c" e "d" deste subitem será feita por declaração do interessado, acompanhada da relação das ações desenvolvidas, mediante diligência do responsável pela licitação.

7.1.3.1.3 Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

a) empresas estabelecidas no Estado da Bahia;

b) empresas brasileiras;

c) empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

d) empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187/2009.

7.1.3.1.4 Se, após observados os subitens 7.1.3.1.2 e 7.1.3.1.3, não houver desempate, será realizado sorteio entre os licitantes, vedando-se qualquer outro critério.

7.1.3.2 Tratando-se de **empate ficto** em relação aos itens de ampla participação:

7.1.3.2.1 O sistema eletrônico identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de se aplicar o disposto nos arts. 44 e 45 da Lei Complementar nº 123/2006.

7.1.3.2.2 Nas condições do subitem 7.1.3.2.1, as propostas de microempresas e empresas de pequeno porte que se encontrarem no intervalo percentual de até 5% (cinco por cento), tratando-se de pregão eletrônico, relativamente à proposta mais bem classificada, serão consideradas empatadas com a primeira colocada (empate ficto).

7.1.3.2.3 A microempresa ou empresa de pequeno porte mais bem classificada, nos termos do subitem 7.1.3.2.2, terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ou em percentual de desconto superior ao da primeira colocada, conforme o critério de julgamento adotado, no prazo de 5 (cinco) minutos controlados pelo sistema eletrônico, contados da comunicação automática.

7.1.3.2.4 Caso a microempresa ou a empresa de pequeno porte mais bem classificada desista ou não se manifeste no prazo estabelecido, o sistema convocará as demais microempresas ou empresas de pequeno porte, em situação de empate ficto, na ordem de classificação, para o exercício do mesmo direito, no mesmo prazo.

7.1.3.2.5 No caso de equivalência dos valores ou dos percentuais de descontos apresentados pelas microempresas e empresas de pequeno porte, conforme o critério de julgamento adotado, que se encontrem nos intervalos percentuais estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

7.1.3.2.6 Se não ocorrer o desempate, prevalecerá a melhor oferta inicial.

7.1.3.3 A realização de **sorteio**, nas hipóteses previstas neste Edital, será realizada em ato público, para o qual os licitantes serão convocados, e do qual será lavrada ata específica.

7.1.3.3.1 Não sendo possível, por razões de ordem operacional, a realização do sorteio por meio do sistema eletrônico, deverá ser designada a realização de ato público presencial, assegurado o acompanhamento e a manifestação por videoconferência ou outro meio idôneo.

7.1.3.3.2 Na hipótese do subitem 7.1.3.3.1, o responsável pela licitação deverá juntar aos autos do processo licitatório no Sistema Eletrônico de Informações – SEI a gravação da sessão pública em áudio e vídeo, nos termos dos §§2º e 5º do art. 17 da Lei Federal nº 14.133/2021.

7.1.3.3.3 O link da gravação, para fins de disponibilização aos interessados, constará de despacho do responsável pela licitação.

Chat para troca de mensagens

7.1.4 Ao final da disputa de lances, o sistema disponibilizará campo próprio para troca de mensagens entre o responsável pela licitação e os licitantes.

Verificação do atendimento às condições de participação

7.1.5 Será procedida à verificação do atendimento às condições de participação, nos termos seguintes:

7.1.5.1 O responsável pela licitação verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei Federal nº 14.133/2021, art. 7º do RLC/PRODEB, legislação correlata e no item 3 do Rito Procedimental deste Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/ceis>);

b) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>);

c) Cadastro de Fornecedores do Estado da Bahia - CAF, mantido pelo Órgão Central do Sistema de Registro Cadastral do Poder Executivo do Estado da Bahia; e

d) Sistema de Cadastramento Unificado de Fornecedores – SICAF.

7.1.5.2 A consulta aos cadastros poderá ser estendida aos administradores e sócios com poderes de administração da licitante, na hipótese de desconsideração da personalidade jurídica a que alude o art. 57 da Lei nº 14.634/2023.

7.1.5.3 Constatada a existência de sanção condenatória restritiva de direito transitada em julgado, nos termos dos arts. 43 e 44 do Decreto nº 23.113/2024, o licitante será excluído da licitação, hipótese em que o responsável pela licitação avaliará a proposta subsequente, na forma do rito estabelecido neste edital.

7.1.5.3.1 A sanção de impedimento de licitar e contratar impedirá o infrator de licitar ou contratar no âmbito da Administração Pública direta e indireta do Estado da Bahia.

7.1.5.3.2 A sanção de declaração de inidoneidade para licitar e contratar impedirá o infrator de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos.

7.1.5.4 O não atendimento das condições de participação importará na exclusão do licitante.

7.1.5.4.1 Na hipótese de exclusão do licitante, o responsável pela licitação avaliará a proposta subsequente, na forma deste edital, e assim, sucessivamente, até a identificação de licitante que atenda às condições de participação.

Readequação da proposta e solicitação de documentos

7.1.6 Por meio do *chat*, o responsável pela licitação solicitará do licitante mais bem classificado, conforme o caso: o envio da proposta readequada ao último lance ofertado; a declaração por ME e EPP de limitação de celebração de

contratos, para fins de obtenção de benefícios da Lei Complementar nº 123/2006; os documentos necessários à avaliação da conformidade da proposta.

7.1.6.1 O responsável pela licitação concederá o prazo de 3 (três) horas para envio dos documentos referidos neste subitem.

7.1.6.2 O prazo definido no subitem 7.1.6.1 poderá ser prorrogado por solicitação fundamentada feita no *chat* pelo licitante, antes de sua conclusão.

7.1.6.3 Em casos justificados, constada a complexidade da proposta, o responsável pela licitação poderá fixar prazo diverso do definido no subitem 7.1.6.1, desde que não superior a 01 (um) dia útil.

7.1.6.4 No caso de licitação em que o procedimento exija apresentação de planilhas com indicação dos quantitativos e dos custos unitários, estas deverão ser encaminhadas pelo sistema com os respectivos valores readequados à proposta provisoriamente classificada em primeiro lugar, sob pena de não aceitação da proposta.

7.1.6.5 Em se tratando de serviços de engenharia, o licitante mais bem classificado deverá apresentar, por meio eletrônico, conforme o critério de julgamento adotado, as planilhas com indicação dos quantitativos e dos custos unitários, seguindo o modelo que integra o TR/Habilitação, bem como com o detalhamento das Bonificações e Despesas Indiretas (BDI) e dos Encargos Sociais (ES), com os respectivos valores readequados ao valor final da proposta provisoriamente classificada em primeiro lugar, na forma disciplinada no TR/Habilitação.

7.1.6.6 A declaração, para fins de obtenção de benefícios da Lei Complementar nº 123/2006, fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, devendo ser firmada, preferencialmente, de acordo com o modelo do formulário integrante deste Edital.

7.1.6.7 Os documentos necessários à avaliação da conformidade da proposta listados no TR/Habilitação compreenderão, dentre outros, os catálogos, manuais, fichas de especificação técnica ou páginas da *internet*.

7.1.6.8 O não envio de qualquer dos documentos por meio do *chat* no prazo indicado pelo responsável pela licitação será considerada desistência, implicando na desclassificação do licitante e à sujeição às sanções administrativas pertinentes.

8. FASE DE JULGAMENTO

8.1 CONTEÚDO APLICÁVEL EXCLUSIVAMENTE AO CRITÉRIO MENOR PREÇO E MAIOR DESCONTO

Adequação da proposta

8.1.1 O responsável pela licitação examinará a proposta do licitante mais bem classificado quanto à compatibilidade do preço ou do desconto e quanto ao atendimento das especificações exigidas.

8.1.1.1 Será desclassificada a proposta que:

- a) conter vícios insanáveis;
- b) não obedecer às especificações técnicas contidas no TR/Habilitação;
- c) apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;
- d) não tiverem sua exequibilidade demonstrada, quando exigido pela PRODEB;
- e) apresentar desconformidade com quaisquer outras exigências deste Edital e/ou seus anexos, desde que insanável.

Avaliação da compatibilidade do preço

8.1.2 O responsável pela licitação aferirá a compatibilidade da proposta em relação ao máximo estipulado para contratação e quanto à sua exequibilidade.

8.1.2.1 Na hipótese de o preço do licitante mais bem classificado superar o limite máximo definido pela PRODEB, o responsável pela licitação poderá negociar a adequação da proposta, a fim de evitar a desclassificação.

8.1.2.1.1 O procedimento de negociação observará o disposto no item 9.

8.1.2.1.2 Quando a proposta do primeiro colocado, mesmo após a negociação, for desclassificada em razão de permanecer acima do preço máximo definido pela PRODEB, deverá ser oportunizada aos demais licitantes a possibilidade de negociação, segundo a ordem de classificação inicialmente estabelecida.

8.1.2.2 No caso de obras e serviços de engenharia e arquitetura, além das disposições eventualmente constantes do TR/Habilitação, a análise de exequibilidade e sobrepreço considerará o que segue:

a) para efeito de avaliação da exequibilidade e de sobrepreço, serão considerados o preço global, os quantitativos e os preços unitários tidos como relevantes, observado o critério de aceitabilidade de preços unitário e global definidos no TR/Habilitação, conforme as especificidades do mercado correspondente (art. 59, §3º, da Lei Federal nº 14.133/2021).

b) serão consideradas inexequíveis as propostas cujos valores forem inferiores a 75% (setenta e cinco por cento) do valor orçado pela PRODEB, independentemente do regime de execução (art. 59, §4º, da Lei Federal nº 14.133/2021).

c) será exigida garantia adicional do licitante vencedor cuja proposta for inferior a 85% (oitenta e cinco por cento) do valor orçado pela PRODEB, equivalente à diferença entre este último e o valor da proposta, sem prejuízo das demais garantias exigíveis de acordo com a Lei Federal nº 14.133/2021 (art. 59, §5º).

8.1.2.3 Se houver indício de inexecuibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos, caberá a realização de diligência, a fim de oportunizar ao licitante a comprovação da exequibilidade da proposta.

8.1.2.4 Não poderá ser considerada exequível a proposta quando os custos do licitante ultrapassem o valor da proposta ou não forem demonstrados custos de oportunidade capazes de justificar a oferta.

Aferição do atendimento às especificações exigidas

8.1.3 Quanto à aferição do atendimento às especificações exigidas, será observado o que se segue:

8.1.3.1 O responsável pela licitação procederá à análise da proposta do licitante mais bem classificado quanto ao atendimento das especificações do objeto, sendo-lhe facultado colher manifestação escrita do setor requisitante do objeto licitado ou da área especializada.

8.1.3.2 Caso previsto no TR/Habilitação, a análise a que se refere o subitem 8.1.3.1 será realizada em procedimento de exame de adequação do objeto, relativamente ao licitante mais bem classificado, compreendendo a apresentação de amostras, avaliação de conformidade, prova de conceito, ou outros testes destinados à aferição da aceitabilidade da proposta, observado o que se segue:

8.1.3.2.1 Será divulgado o local e horário de realização do procedimento de exame de adequação do objeto, o qual deverá ser atendido pelo licitante, sob pena de preclusão.

8.1.3.2.2 A divulgação será feita por mensagem no sistema eletrônico, no sítio eletrônico oficial ou por outro meio idôneo, com a antecedência necessária para a sua realização.

8.1.3.2.3 Não sendo possível, por razões de ordem operacional, a permissão à participação presencial dos interessados na realização do exame de adequação do objeto, deverá ser assegurado o acompanhamento e a manifestação no ato, por videoconferência ou outro meio idôneo.

8.1.3.2.4 A recusa do licitante à realização do exame de adequação do objeto ou atraso, sem justificativa aceita pelo responsável pela licitação, de entrega da amostra, realização do exame de conformidade, de prova de conceito ou de outros testes exigidos será considerada desistência do certame, ensejando a aplicação das penalidades pertinentes.

8.1.3.2.5 O objeto será considerado inadequado, quando verificado o não atendimento das especificações previstas neste Edital.

8.1.3.2.6 Os resultados das avaliações serão divulgados pelos meios previstos no subitem 8.1.3.2.2.

8.1.3.2.7 Durante o prazo de vigência do contrato ou da ata de registro de preços, o Contratante/ gerenciador da ata de RP poderá, justificadamente, exigir amostra ou prova de conceito do bem (art. 41, inc. II, da Lei Federal nº 14.133/2021 e art. 133, XVI do RLC/PRODEB).

Documentos complementares à proposta de preço

8.1.4 Caso seja necessário, o responsável pela licitação poderá, em sede de diligência, solicitar documentos complementares à proposta **de preço**, a fim de esclarecer ou confirmar situação fática ou jurídica pré-existente (art. 36 do Decreto nº 22.888/2024 e art. 82, §4º do RLC/PRODEB).

8.1.4.1 Na realização de diligência, o responsável pela licitação deverá atentar para o caráter de complementaridade das informações e documentos a serem juntados (art. 36, parágrafo único, do Decreto nº 22.888/2024).

8.1.4.2 Não serão aceitos documentos ou informações que devessem constar originariamente da proposta.

8.1.4.3 O não envio dos documentos complementares no prazo indicado pelo responsável pela licitação será considerada desistência, implicando na desclassificação do licitante e à sujeição às sanções administrativas pertinentes.

Sanatória da proposta

8.1.5 O responsável pela licitação poderá sanar erros ou falhas que não alterem a substância da proposta, mediante despacho fundamentado registrado e acessível a todos, atribuindo-lhes eficácia para fins de classificação (art. 37 do Decreto nº 22.888/2024 e art. 68, §6º do RLC/PRODEB).

Providências ulteriores

8.1.6 No caso de desclassificação, o responsável pela licitação avaliará a proposta subsequente, de acordo com a disciplina estabelecida no rito estabelecido neste edital, procedendo a nova verificação da ocorrência do empate ficto, se for o caso, de acordo com a disciplina estabelecida, e assim sucessivamente, até a obtenção de proposta válida.

8.1.7 Não sendo possível o julgamento da proposta na mesma sessão, o responsável pela licitação deverá designar nova sessão, para a qual serão convocados os licitantes.

8.1.8 A fase de julgamento será encerrada com a identificação do licitante classificado detentor da melhor proposta.

9. NEGOCIAÇÃO

9.1. Definido o resultado do julgamento, o responsável pela licitação poderá negociar condições mais vantajosas com o licitante classificado detentor da melhor proposta.

9.1.1 A negociação será conduzida pelo responsável pela licitação por meio do sistema eletrônico, podendo ser acompanhada pelos demais licitantes.

9.1.2 O resultado da negociação será registrado na ata da sessão pública, divulgado a todos os licitantes e anexado aos autos do processo licitatório.

9.1.3 Concluída a negociação, o responsável pela licitação solicitará o envio da proposta readequada, observado o disposto no subitem 7.

10. FASE DE HABILITAÇÃO

Documentos de habilitação

10.1 Para habilitação dos licitantes, serão exigidos os documentos necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, nos termos dos arts. 62 a 70 da Lei Federal nº 14.133/2021 e arts. 91 a 101 do RLC/PRODEB, conforme definido no TR/Habilitação, dividindo-se em: jurídica; técnica; fiscal, social e trabalhista (quando cabível); e econômico-financeira.

10.1.1 A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira poderá ser substituída pelo Certificado de Registro Cadastral do Cadastro de Fornecedores do Estado da Bahia (CAF) ou SICAF quanto aos documentos por ele abrangidos, observado o disposto neste Edital.

10.1.2 Os documentos exigidos para fins de habilitação observarão os termos da Lei Federal nº 13.726, de 8 de outubro de 2018.

10.1.3 Na forma do art. 63, inc. I, da Lei Federal nº 14.133/2021 e do RLC/PRODEB, o licitante responderá pela veracidade das declarações a que se refere o subitem 4.3.

10.1.4 Somente haverá a necessidade de apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

Microempresas e empresas de pequeno porte

10.2 A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte observará o disposto no art. 43 da Lei Complementar nº 123/2006.

10.2.1 O responsável pela licitação procederá à verificação se a microempresa ou empresa de pequeno porte faz jus aos benefícios da Lei Complementar nº 123/2006, em conformidade com os termos definidos neste Edital.

Empresas estrangeiras

10.3 Quando permitida a participação de empresas estrangeiras que não funcionem no País, será observado o que segue:

10.3.1 As exigências de habilitação serão atendidas mediante documentos equivalentes inicialmente apresentados com tradução livre;

10.3.2 O licitante deverá ter procurador residente e domiciliado no país, com poderes para receber citação, intimação e responder administrativa e judicialmente por seus atos, juntando os instrumentos de mandato com os demais documentos de habilitação;

10.3.3 Para fins de assinatura do contrato ou da ata de registro de preços, os documentos de que trata este artigo serão traduzidos por tradutor juramentado no país e apostilados ou consularizados pelos respectivos consulados ou embaixadas.

Consórcio de empresas

10.4 Salvo vedação devidamente justificada no TR/Habilitação, pessoa jurídica poderá participar de licitação em consórcio, observado o disposto no art. 15 e nos §§10 e 11 do art. 67, todos da Lei Federal nº 14.133/2021 e art. 104 do RLC/PRODEB.

10.4.1 Quando houver a participação de consórcio de empresas, a habilitação técnica, se exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

Processamento da habilitação

10.5 Serão exigidos os documentos de habilitação apenas do licitante classificado detentor da melhor proposta, exceto na inversão de fases (art. 63, inc. II, da Lei Federal nº 14.133/2021 e art. 42, § único do RLC/PRODEB).

10.5.1 Quando houver inversão de fases, a exigência dos documentos de habilitação ocorrerá em relação a todos os licitantes.

10.5.2 Excetuam-se da previsão deste subitem os documentos relativos à regularidade fiscal, os quais serão exigidos, quando couber, em momento posterior ao julgamento das propostas e somente do licitante classificado detentor da melhor proposta (art. 63, inc. III, da Lei Federal nº 14.133/2021).

10.6 Os documentos de habilitação serão enviados por meio do sistema eletrônico, em formato digital, no prazo 3 (três) horas, prorrogável por prazo não superior a 01 (um) dia útil, contado da solicitação do responsável pela licitação.

10.6.1 Na hipótese de inversão de fases, os licitantes encaminharão simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto.

10.6.2 Em caso de falhas técnicas ou operacionais que inviabilizem o envio de documentação de que trata este subitem 10.6, será admitido o envio correspondente para o correio eletrônico (e-mail) indicado no Preâmbulo deste Edital, devendo o responsável pela licitação informar no *chat* do sistema eletrônico a data e o horário do seu recebimento, disponibilizando o seu conteúdo, em seguida, para os demais licitantes.

10.7 A habilitação poderá ser verificada por meio do CAF, quanto aos documentos por ele abrangidos, exceto quanto aos documentos de qualificação técnica.

10.7.1 Os documentos exigidos para habilitação que não estejam contemplados no CAF, ou que dele constem como vencidos, ou que não possam ser substituídos pelo certificado, deverão ser apresentados pelo licitante, na forma prevista neste Edital.

10.7.2 Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

10.8 Nas licitações restritas a fornecedores cadastrados, a habilitação será verificada por meio do CAF, observado o disposto no subitem 10.6.

10.9 É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no CAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo solicitar a modificação dos registros em caso de incorreção.

10.10 A verificação, pelo responsável pela licitação, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões, constitui meio legal de prova, para fins de habilitação.

10.10.1 Desde que solicitado de forma expressa pelo licitante interessado, e sob sua inteira e exclusiva responsabilidade, inclusive no que respeita à adequação da habilitação econômico-financeira e da qualificação técnica, a documentação de habilitação enviada para determinado lote poderá ser utilizada para fins de avaliação da habilitação em outro lote no qual o licitante tenha sido o melhor classificado.

Documentos complementares à habilitação

10.11 Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (art. 64 da Lei Federal nº 14.133/2021 e art. 82, §4º do RLC/PRODEB):

a) complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

b) atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

10.11.1 Os documentos serão enviados por meio do sistema eletrônico, em formato digital, no prazo 3 (três) horas, prorrogável por igual período, contado da solicitação do responsável pela licitação, observado o disposto no subitem 10.5.

10.11.2 O não envio dos documentos complementares no prazo indicado será considerada desistência, implicando na inabilitação do licitante e à sujeição às sanções administrativas pertinentes.

Sanatória

10.12 Na análise dos documentos de habilitação, o responsável pela licitação poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação (art. 64, §1º da Lei Federal nº 14.133/2021 e art. 68, §6º do RLC/PRODEB).

10.12.1 Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

Comprovação dos requisitos de habilitação diferidos

10.13 O responsável pela licitação definirá o prazo para a apresentação dos requisitos de habilitação cuja exigência tenha sido diferida.

10.13.1 A não apresentação da documentação no prazo definido, implicará inabilitação do licitante e sujeição às sanções administrativas pertinentes.

10.14 Tratando-se de microempresa ou empresa de pequeno porte, beneficiária do regime diferenciado da Lei Complementar nº 123/06, cuja participação tenha sido realizada com a ressalva de existência de restrição fiscal e/ou trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que a proponente for declarada a vencedora do certame, prorrogável por igual período, a critério da PRODEB, para a

regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa

10.14.1 A não-regularização da documentação no prazo previsto neste item implicará decadência do direito à contratação e inabilitação do licitante, além da sujeição às sanções administrativas pertinentes, na forma do disposto no §2º do art. 53 da Lei Complementar nº 123/06.

Inabilitação

10.15 Na hipótese de o licitante não atender às exigências de habilitação, o responsável pela licitação examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda aos requisitos e especificações, procedendo, inclusive, a nova verificação da ocorrência do empate ficto, na forma prevista neste Edital.

Encerramento da fase de Habilitação

10.16 Não sendo possível o julgamento da habilitação na mesma sessão, o responsável pela licitação deverá designar nova sessão, observado o prazo mínimo de 24h (vinte e quatro horas), para a declaração do licitante provisoriamente vencedor, para a qual ficarão convocados os licitantes.

10.17 Exceto na inversão de fases, encerrada a fase de habilitação, será declarado o licitante provisoriamente vencedor, ato do qual ficarão automaticamente intimados os licitantes.

11. IMPUGNAÇÃO AO EDITAL E PEDIDO DE ESCLARECIMENTO

11.1 Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade ou para solicitar esclarecimentos sobre os seus termos, devendo encaminhar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

11.1.1 A impugnação e o pedido de esclarecimento serão realizados na forma eletrônica.

11.2 O responsável pela licitação responderá aos pedidos de esclarecimentos e impugnação no prazo de até 03 (três) dias úteis contado da data de recebimento do pedido, limitado ao último dia útil anterior à data da abertura do certame, e poderá requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos seus anexos.

11.2.1 O responsável pela licitação poderá solicitar a manifestação dos setores técnicos do órgão ou entidade contratante, a fim de subsidiar as decisões de caráter técnico, conforme o §3º do art. 8º do Decreto nº 22.885/2024 e a oitiva, quando necessário, dos órgãos de assessoramento jurídico e de controle interno, nos termos do art. 32 do Decreto nº 22.885/2024.

11.3 A impugnação não possui efeito suspensivo, sendo a sua concessão medida excepcional que deverá ser motivada pelo responsável pela licitação nos autos do processo de licitação.

11.4 Acolhida a impugnação contra o edital de licitação, será definida e publicada nova data para realização do certame, devendo ser observado o disposto no subitem 17.12

11.5 A resposta à impugnação ou ao pedido de esclarecimento será divulgada no endereço eletrônico www.comprasnet.ba.gov.br e no <https://licitacoes-e2.bb.com.br/aop-inter-estatico/>, no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame, e vincularão os participantes e a PRODEB.

12. FASE RECURSAL

12.1 A fase recursal obedecerá à disciplina estabelecida neste Edital, observado o disposto no art. 165 da Lei Federal nº 14.133/2021 e art. 227 do RLC/PRODEB.

12.2 Dos atos decorrentes do procedimento licitatório, cabem:

12.2.1 Recurso:

a) em fase única, em face do julgamento das propostas e do ato de habilitação ou inabilitação;

b) em face do ato de anulação ou revogação da licitação.

12.2.2 Pedido de reconsideração, relativamente a ato do qual não caiba recurso hierárquico.

12.3 O recurso em face do julgamento das propostas e do ato de habilitação ou inabilitação observará as seguintes disposições:

12.3.1 A intenção de recorrer deverá ser manifestada imediatamente, no prazo de 15 (quinze) minutos, sob pena de preclusão, após a declaração do licitante provisoriamente vencedor pelo responsável pela licitação.

12.3.1.1 A manifestação da intenção de recorrer será única, abrangendo as matérias concernentes ao julgamento das propostas e ao ato de habilitação ou inabilitação.

12.3.2 Manifestada a intenção de recorrer, as razões de recurso deverão ser apresentadas no prazo de 3 (três) dias úteis, contado da data de intimação da declaração do licitante provisoriamente vencedor.

12.3.3 O prazo para apresentação de contrarrazões será de 3 (três) dias úteis, contado da data de divulgação da interposição do recurso, a qual será feita por comunicação no *chat*.

12.3.4 O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, para juízo de retratação.

- 12.3.4.1 Se a autoridade não reconsiderar o ato ou a decisão no prazo de 3 (três) dias úteis, encaminhará o recurso com a sua motivação à autoridade superior.
- 12.3.5 A autoridade superior deverá proferir sua decisão no prazo máximo de 3 (dez) dias úteis, contado do recebimento dos autos, nos termos do art. 231 do RLC/PRODEB.
- 12.3.6 O acolhimento do recurso implicará invalidação apenas de ato insuscetível de aproveitamento.
- 12.3.7 Os recursos interpostos fora do prazo não serão conhecidos.
- 12.3.8 O resultado dos recursos será divulgado no endereço eletrônico www.comprasnet.ba.gov.br.
- 12.4 Aplica-se o disposto no subitem 12.3, no que couber, ao recurso em face do ato de anulação ou revogação da licitação.
- 12.5 O pedido de reconsideração será apresentado no prazo de 3 (três) dias úteis, contado da data de intimação, observado o inc. II do art. 165 da Lei Federal nº 14.133/2021.
- 12.6 O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.
- 12.6.1 Na elaboração de suas decisões, a autoridade competente será auxiliada pelo órgão de assessoramento jurídico, que deverá dirimir dúvidas e subsidiá-la com as informações necessárias.
- 12.7 Será assegurado ao licitante vista dos elementos indispensáveis à defesa de seus interesses.

13. ADJUDICAÇÃO E HOMOLOGAÇÃO

- 13.1 Encerradas as fases de julgamento e habilitação, e exauridos os recursos administrativos, o processo licitatório será encaminhado à autoridade superior, que poderá:
- a) determinar o retorno dos autos para saneamento de irregularidades;
 - b) revogar a licitação por motivo de conveniência e oportunidade;
 - c) proceder à anulação da licitação, de ofício ou mediante provocação de terceiros, sempre que presente ilegalidade insanável;
 - d) adjudicar o objeto e homologar a licitação.
- 13.1.1 Ao pronunciar a nulidade, a autoridade indicará expressamente os atos com vícios insanáveis, tornando sem efeito todos os subsequentes que deles dependam, e dará ensejo à apuração de responsabilidade de quem lhes tenha dado causa.
- 13.1.2 O motivo determinante para a revogação do processo licitatório deverá ser resultante de fato superveniente devidamente comprovado.
- 13.1.3 Nos casos de anulação e revogação, deverá ser assegurada a prévia manifestação dos interessados.
- 13.1.4 Havendo justo receio de prejuízo de difícil ou incerta reparação decorrente do ato de anulação e revogação, poderá ser diferida a manifestação dos interessados, com fundamento no art. 183 da Lei nº 12.209, de 20 de abril de 2011, justificadamente.
- 13.2 A homologação da licitação não implicará direito à contratação.

14. CONTRATAÇÃO

Convocação para assinatura

- 14.1 Após a homologação, o licitante vencedor será convocado para assinar o termo de contrato ou, nas hipóteses previstas no art. 95 da Lei Federal nº 14.133/2021 e art. 139 do RLC/PRODEB, o instrumento hábil que lhe substitua: Autorização de Fornecimento de Material - AFM ou Autorização de Prestação de Serviços - APS, conforme o caso, no prazo estabelecido no Preâmbulo deste Edital, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas na Lei Federal nº 14.133/2021 e RLC/PRODEB, e em outras legislações aplicáveis.
- 14.1.1 O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do adjudicatário durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela PRODEB.
- 14.1.2 A contratação obedecerá as estipulações constantes da minuta de contrato integrante do edital da licitação, do aviso ou do instrumento de contratação direta.
- 14.1.3 Na hipótese de substituição do termo de contrato por instrumento equivalente, neste serão consideradas literalmente transcritas todas as cláusulas e condições previstas na minuta de contrato constante deste Edital.
- 14.1.4 O termo de contrato, a AFM ou, a APS, conforme o caso, deve ser assinado pelo representante legal do licitante ou mandatário com poderes expressos.
- 14.1.5 A assinatura se dará por meio do Sistema Eletrônico de Informações - SEI, caso em que o licitante deverá providenciar o cadastramento de seu representante legal ou procurador no endereço eletrônico www.portalseibahia.saeb.ba.gov.br ou através do link disponibilizado www.comprasnet.ba.gov.br.
- 14.2. Será facultado à PRODEB, observados os tramites pactuados no Termo de Cooperação Técnica nº 002/2026, quando o convocado não assinar o termo de contrato, AFM ou APS, conforme o caso, no prazo e nas condições estabelecidas, convocar os licitantes remanescentes, na ordem de classificação, para a celebração do contrato nas condições propostas pelo licitante vencedor.

14.3 Decorrido o prazo de validade da proposta indicado neste Edital, sem convocação para a contratação, ficarão os licitantes liberados dos compromissos assumidos.

14.4 Na hipótese de nenhum dos licitantes aceitar a contratação nos termos do subitem 14.2 a PRODEB, observados o valor estimado e sua eventual atualização nos termos deste edital, poderá:

a) convocar os licitantes remanescentes para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário, mas não superior ao preço ofertado pelo próprio licitante remanescente;

b) adjudicar e celebrar o contrato nas condições ofertadas pelos licitantes remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

14.5. A negociação a que se refere a alínea "a" do subitem 14.4 deste artigo deverá ser oportunizada aos licitantes remanescentes, assegurada a preferência, em caso de empate, ao licitante mais bem classificado.

Recusa

14.6 A recusa injustificada do adjudicatário em assinar o termo de contrato, AFM ou APS, conforme o caso, no prazo estabelecido pela PRODEB, dentro do prazo de validade da proposta, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas e à imediata perda da garantia de proposta em favor do órgão ou entidade promotor da licitação (art. 90, §5º, c/c art. 155, inc. VI, da Lei Federal nº 14.133/2021 e art. 211, VI do RLC/PRODEB).

14.7 Equipara-se à recusa prevista no subitem 14.6 a circunstância de o adjudicatário deixar de manter as condições de habilitação exigidas na licitação, ou, por qualquer meio, dar causa à impossibilidade de celebrar o contrato.

14.8 A multa compensatória para a recusa injustificada do adjudicatário em assinar o termo de contrato, em aceitar ou retirar o instrumento equivalente, ou praticar condutas a elas equiparadas, corresponderá, salvo previsão diversa, ao mesmo percentual definido para o descumprimento total da obrigação principal, e incidirá sobre o valor global do contrato (art. 8º, §§1º e 4º, do Decreto nº 23.113/2024).

14.8.1 Nas hipóteses em que não houver valor contratado, a sanção de multa terá como base o valor correspondente ao objeto adjudicado ou, quando for o caso, da estimativa da contratação (art. 7º, §1º, c/c art. 8º, §4º, do Decreto nº 23.113/2024).

14.9 A regra do subitem 14.6 não se aplicará aos licitantes remanescentes convocados na forma da alínea "a" do subitem 14.4, **exceto** se estes passarem à condição de licitante adjudicatário (art. 48, §8º, do Decreto nº 22.888/2024).

15. INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

15.1 Constituem infrações administrativas para os fins deste Edital as condutas constantes do art. 155 da Lei Federal nº 14.133/2021 (art. 47 da Lei nº 14.634/2023) e art. 211 do RLC/PRODEB.

15.2 Os licitantes estarão sujeitos às sanções administrativas referidas na Lei nº 14.634/2023 e RLC/PRODEB, e às demais cominações legais, resguardado o direito à ampla defesa e ao contraditório.

16. DISPOSIÇÕES DO SISTEMA DE REGISTRO DE PREÇOS

16.1 Tratando-se de licitação destinada ao Sistema de Registro de Preços, serão observados, ainda, os acréscimos da **Seção do Sistema do Registro de Preços – SRP**, os quais prevalecerão em caso de conflito.

17. DISPOSIÇÕES FINAIS

17.1 A ata da sessão pública será divulgada no sistema eletrônico.

17.2 Os horários estabelecidos neste Edital, no aviso da licitação e durante a sessão pública observarão o horário de Brasília, Distrito Federal, inclusive para contagem de tempo e prática de atos processuais.

17.3 As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da PRODEB, os princípios elencados no art. 5º da Lei Federal nº 14.133/2021 e art. 3º do RLC/PRODEB, a finalidade e a segurança da contratação.

17.4 Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a PRODEB não será responsável por quaisquer custos, independentemente da condução ou do resultado do processo licitatório.

17.5 Na contagem dos prazos estabelecidos neste Edital observar-se-á o art. 183 da Lei Federal nº 14.133/2021 e art. 8º, §4º do RLC/PRODEB.

17.6 Os atos de comunicação processual da PRODEB com os licitantes serão realizados por meio eletrônico, na forma do disposto na Lei nº 12.209/2011 e no Decreto nº 15.805, de 30 de dezembro de 2014.

17.6.1. A Contratada deverá manter atualizado o endereço eletrônico cadastrado no Sistema Eletrônico de Informações - SEI, para efeito do recebimento de notificação e intimação de atos processuais, conforme Decreto nº 17.983, de 24 de outubro de 2017, devendo atender às convocações da PRODEB para a prática de atos nos prazos indicados.

17.7 A autoridade competente poderá, até a assinatura do contrato, excluir licitante, em despacho motivado, se tiver ciência de fato ou circunstância, anterior ou posterior ao julgamento da licitação, que revele inidoneidade ou falta de

capacidade técnica ou financeira para a execução do contrato, assegurada a manifestação do interessado (art. 66 da Lei nº 14.634/2023 e art. 91, I do RLC/PRODEB).

17.8 Eventuais modificações neste Edital implicarão nova divulgação na mesma forma de sua divulgação inicial, além do cumprimento dos mesmos prazos dos atos e procedimentos originais, exceto se, inquestionavelmente, a alteração não comprometer a formulação das propostas, resguardado o tratamento isonômico aos licitantes.

17.9 Os casos omissos serão dirimidos pelo Órgão/Entidade indicados no Preâmbulo deste Edital, segundo as disposições contidas no Regulamento de Licitações e Contratos da PRODEB, na Lei Federal nº 14.133/2021, na Lei nº 14.634/2023, e demais normas aplicáveis.

18. FORO

18.1 As partes elegem o Foro da Cidade do Salvador, Estado da Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para solucionar quaisquer dúvidas oriundas deste instrumento que não puderem ser dirimidas por quaisquer dos meios alternativos de resolução de controvérsias de que trata o Regulamento de Licitações e Contratos da PRODEB e a Lei Federal nº 14.133/2021.

SEÇÃO II – ESPECIFICAÇÕES DO SISTEMA DE REGISTRO DE PREÇOS

1. DISPOSIÇÕES GERAIS

O registro de preços observará o RLC/PRODEB, o Decreto nº 23.657/2025 e o disposto nesta Seção.

1.1. A existência de preços registrados implicará compromisso de fornecimento, pelo fornecedor com preço registrado, nas condições estabelecidas, mas não obrigará a PRODEB a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente motivada e autorizada pela autoridade competente (art. 5º).

1.1.1 Na hipótese de registro de preços para compra interfederativa, a não utilização da contratação disponibilizada pela ata de registro de preços deverá estar prevista expressamente no ato normativo ou no instrumento que disciplinar a cooperação (art. 5º, parágrafo único).

2. DEFINIÇÕES

Para os fins do disposto nesta Seção, serão consideradas as definições do art. 2º do Decreto nº 23.657/2025.

3. CRITÉRIO DE JULGAMENTO

Na licitação para registro de preços, será adotado o critério de julgamento de menor preço ou de maior desconto, conforme indicado no preâmbulo deste edital, observado o disposto no art. 14 do Decreto nº 23.657/2025.

3.1 O critério de aceitabilidade de preços unitários máximos é o constante do Termo de Referência e Habilitação (TR/Habilitação).

4. ADEQUAÇÃO DO PREÇO

Em nenhuma hipótese serão registrados na ata ou admitidos no cadastro de reserva preços incompatíveis com os preços praticados no mercado ou fixados pela PRODEB ou por órgão oficial competente ou constantes de tabela de preços referenciais (art. 17).

5. DO CADASTRO DE RESERVA

Formação do cadastro de reserva (art. 19)

5.1 Na licitação para registro de preços, haverá a etapa da formação do cadastro de reserva, o qual terá como objetivo possibilitar a substituição do adjudicatário ou do fornecedor com preço registrado, nas hipóteses admitidas.

5.1.1 Declarado o vencedor e exauridos os recursos administrativos, o responsável pela licitação facultará a todos os licitantes a possibilidade de integrar o cadastro de reserva.

5.1.1.1 Para as providências de que trata o subitem 5.1.1 deverá ser adotado, no que couber, os mesmos ritos e prazos definidos neste Edital.

5.1.2 O cadastro de reserva conterá o registro:

I - dos licitantes que aceitarem cotar os itens em preços iguais aos do licitante vencedor na sequência de classificação no procedimento; e

II - dos licitantes que mantiverem sua proposta.

5.1.3 Para fins da ordem de classificação, e desde que observado o disposto no item 4 desta Seção, os fornecedores de que trata o inciso I do subitem 5.1.1 antecederão aqueles de que trata o inciso II do mesmo subitem.

5.1.4 Não poderão compor o cadastro de reserva as propostas que não tenham sido classificadas e cujos licitantes não tenham sido habilitados.

5.1.5 Na hipótese de substituição do adjudicatário ou do fornecedor com preço registrado ou, ainda, de modificação do preço registrado em decorrência de reajustamento, repactuação ou alteração, poderá ser procedida à reorganização do cadastro de reserva, mediante a reclassificação dos seus integrantes. (art. 19, §3º, inciso II)

Acionamento do cadastro de reserva (art. 20)

5.2 Ressalvada a existência de previsão específica nesta Seção ou na ata de registro de preços, o acionamento do cadastro de reserva consistirá na adoção das seguintes providências, sucessivamente, até a identificação do substituto do adjudicatário ou do fornecedor com preço registrado, conforme o caso:

I - na convocação dos licitantes referidos no inciso I do subitem 5.1.1, na ordem de classificação, visando à manutenção do mesmo preço;

II – na convocação dos licitantes referidos no inciso II do subitem 5.1.1, na ordem de classificação, para:

- a) manifestar se aceitam praticar o mesmo preço do adjudicatário ou do fornecedor com preço registrado;
- b) negociar preço melhor, mesmo que acima do preço do adjudicatário ou do fornecedor com preço registrado e inferior ao que fora ofertado pelo próprio licitante.

5.2.1 Quando frustrada a negociação de melhor condição referida na alínea “b” do inciso II deste subitem, poderá ser procedida à substituição com base nas condições que haviam sido ofertadas pelo próprio licitante integrante do cadastro de reserva.

5.2.2 A aceitação da substituição a que se refere o item 5.2 será facultativa, exceto na hipótese de o integrante do cadastro de reserva passar à condição de adjudicatário, caso em que será observado o disposto no subitem 6.3 desta Seção.

5.2.2.1 Uma vez subscrita a ata de registro de preços, o substituto a ela se obriga, na qualidade de fornecedor com preço registrado.

5.2.3 Aplica-se o disposto neste item na hipótese de contratação de remanescente de obra, de serviço ou de fornecimento em consequência de rescisão contratual (art. 90, §7º, da Lei nº 14.133/2021 e art. 138, §2º do RLC/PRODEB).

6. ATA DE REGISTRO DE PREÇOS

Confeção da Ata de Registro de Preços (art. 21)

6.1 Após a homologação da licitação, será confeccionada a ata de registro de preços, contemplando as informações previstas no inciso II do art. 2º Decreto nº 23.657/2025.

6.1.1 A ata de registro de preços obedecerá as condições da minuta anexa a este Edital.

Assinatura da Ata de Registro de Preços (art. 22)

6.2 Será procedida à convocação do adjudicatário para assinatura da ata de registro de preços no prazo e nas condições estabelecidas no Preâmbulo deste Edital, sob pena de decadência do direito, sem prejuízo da aplicação das sanções legalmente previstas.

6.2.1 O prazo de convocação poderá ser prorrogado uma vez, por, no máximo, idêntico período, mediante solicitação tempestiva do interessado, desde que motivada e aceita pela PRODEB.

6.2.2 A recusa injustificada do adjudicatário em assinar a ata, dentro do prazo de validade da proposta, ensejará a aplicação das penalidades legalmente estabelecidas.

6.2.3 Equipara-se à recusa prevista no subitem 6.2.2 a circunstância de o adjudicatário do registro de preços deixar de manter as condições de habilitação exigidas na licitação ou no procedimento de contratação direta, ou, por qualquer meio, dar causa à impossibilidade de subscrição da ata.

6.2.4 A multa compensatória para a recusa injustificada do adjudicatário em assinar a ata de registro de preços, ou praticar condutas a elas equiparadas, corresponderá, salvo previsão diversa, à metade do percentual definido para o descumprimento total da obrigação principal, e terá como base o valor correspondente ao objeto adjudicado ou, quando for o caso, da estimativa da contratação (art. 7º, §1º c/c art. 8º, §§2º e 4º do Decreto nº 23.113/2024).

Acionamento do cadastro de reserva em decorrência da recusa à assinatura da ata (art. 23)

6.3 Quando o adjudicatário não assinar a ata de registro de preços no prazo e condições estabelecidos, é facultado à PRODEB o acionar o cadastro de reserva, na forma prevista no subitem 5.2 desta Seção.

6.3.1 No procedimento referido neste item, deverá ser observado o disposto no subitem 6.2 desta Seção, inclusive quanto à aplicação de penalidades, em caso de recusa à assinatura da ata, dentro do prazo de validade da proposta, pelos integrantes do cadastro de reserva sucessivamente convocados a substituir o adjudicatário.

Divulgação (art. 24)

6.4 A ata de registro de preços deverá ser divulgada no PNCP, sem prejuízo da divulgação adicional no sítio eletrônico oficial utilizado pelo órgão ou entidade gerenciadora.

6.4.1 O preço registrado, com indicação do respectivo fornecedor, será divulgado e mantido no sítio eletrônico oficial, durante a vigência da ata de registro de preços.

6.4.2 Qualquer cidadão é parte legítima para impugnar preço constante do registro, em razão da sua incompatibilidade com o preço praticado no mercado.

6.4.3 Deverá ser realizada periódica pesquisa de mercado para comprovação da vantajosidade dos preços registrados.

ANEXO I – TERMO DE REFERÊNCIA

OBSERVAÇÃO: DEVIDO AO TAMANHO DO ARQUIVO O TERMO DE REFERÊNCIA E SEUS ANEXOS SE ENCONTRAM EM APENSO A ESTE EDITAL.

ANEXO II – MINUTA DE ATA DE REGISTRO DE PREÇOS

Modalidade de Licitação	Número

A COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DA BAHIA-PRODEB, sociedade de economia mista, com sede nesta Capital na Avenida Quatro, Nº 410 - Centro Administrativo da Bahia, inscrita no CNPJ sob o Nº 13.579.586/0001-32, neste ato representada pelos seus Diretores Executivo e de Infraestrutura Tecnológica e Conectividade, Srs. José Muniz Rebouças e Carlos Augusto Borges Silva, doravante denominada simplesmente **PRODEB**, e a proponente XXXXXXXXXXXXXXXXXXXX, CNPJ nº XXXXXXXXXXXXXXXX, Inscrição Estadual nº XXXXXXXX /Municipal nº XXXXXX, situada à XXXXXXXXXXXXXXXXXXXXXXXX, CEP: XXXXXXXXXXXXX, Cidade XXXXXXXXXXX, neste ato representada pela Sr. (a) XXXXXXXXXXXX, portador (a) da cédula de identidade nº XXXXXXXXXXXXXXXX, emitida por XXXXXXXXXXXXXXXX, inscrito (a) no CPF/MF sob o nº XXXXXXXXXXXXXXXX, doravante denominado **FORNECEDOR**, em decorrência do rito similar ao Pregão Eletrônico nº 005/2026, processo administrativo SEI nº 065.10933.2026.0003946-61, firmam a presente **ATA DE REGISTRO DE PREÇOS**, em proveito da PRODEB e demais participantes originários da presente ata nos termos do Anexo IV do Termo de Referência, que se regerá pela Lei Federal nº 13.303/2016 e pelo Regulamento de Licitações e Contratos - RLC da PRODEB, aprovado pelo CAD em 29/06/2018, alterado em 18/06/2024 e subsidiariamente, pelas Leis nºs 14.133/2021 e 14.634/2023, bem como pela Lei Complementar nº 123/2006 e suas alterações, da Lei Federal nº 13.709/2018, do Decreto Estadual nº 22.886/2024, do Decreto Estadual nº 22.888/2024, do Decreto Estadual nº 23.113/2024, do Decreto Estadual nº 23.356/2025, do Decreto Estadual nº 23.657/2025, do Decreto Estadual nº 24.318/2026 e respectivas alterações e demais legislações pertinentes, mediante as cláusulas e condições a seguir ajustadas:

1. FINALIDADE DA ATA/ OBJETO

1.1 Esta ata de registro de preços constitui documento vinculativo e obrigacional, com característica de compromisso para futura contratação com o fornecedor, no qual são registrados o objeto, os preços, os quantitativos, os participantes e as condições a serem praticadas, conforme as disposições contidas no Termo de Referência (TR) e da proposta apresentada pelo licitante (art. 2º, inciso II do Decreto 23.657/2025).

1.2 A presente Ata tem por objeto o registro de preços para eventual contratação de empresa especializada em **solução de conectividade segura, incluindo proteção de borda, firewall de próxima geração, links de internet e solução de operação e monitoramento central, pelo período de 60 meses e soluções de segurança da informação e cibersegurança, compreendendo licenciamento, atualização, garantia e demais serviços associados, pelo período de 12 meses**, descritos no Termo de Referência do Edital de Pregão Eletrônico nº 005/2026, o qual integra este instrumento para todos os fins, bem como das propostas cujos preços tenham sido registrados, independentemente de transcrição, conforme disposto a seguir:

LOTE 01: Solução de conectividade segura, incluindo proteção de borda, firewall de próxima geração (NGFW) com tecnologia SD-WAN, links de internet e Solução de Operação e Monitoramento Central, pelo período de 60 meses; Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço, conforme especificações técnicas detalhadas no Termo de Referência.

LOTE 02: Soluções de segurança da informação e cibersegurança, compreendendo equipamentos de firewall, licenciamento, atualização, garantia e serviços de upgrade, voltados à proteção dos ambientes tecnológicos, das comunicações de dados e das aplicações corporativas dos órgãos e entidades do Poder Executivo Estadual, pelo período de 12 meses, conforme especificações técnicas detalhadas no Termo de Referência.

2. ÓRGÃO OU ENTIDADE GERENCIADOR

2.1 A Companhia de Processamento de Dados do Estado da Bahia – PRODEB é a gestora da Ata de Registro de Preços, sendo responsável pelo controle de vigência, saldos, registros e demais aspectos operacionais da Ata. A liberação de contratações, saques, adesões ou utilizações dos itens registrados ficará condicionada à prévia e expressa autorização da Secretaria da Administração – SAEB, conforme estabelecido no item 11.4 do TR.

3. PRAZO DE VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

3.1 A Ata de Registro de Preços terá vigência inicial de 01 (um) ano, podendo ser prorrogada por igual período, desde que comprovada a vantajosidade do preço, com renovação integral dos quantitativos para o novo período, conforme o art. 18 do Decreto Estadual nº 23.657/2025 e art. 137 do RLC/PRODEB, conforme estabelecido no item 11.12 do TR.

4. PREÇO

4.1 Os preços registrados, as especificações do objeto, as quantidades de cada item, fornecedor(es) e as demais condições ofertadas encontram-se adiante especificados no demonstrativo que segue:

LOTE 01							
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor mensal unitário (R\$) A	Valor unitário para 60 meses (R\$) B = A * 60	Valor Total 60 meses (R\$) C = B * QTD
1	02.81.00.00192352-8	Solução de Conectividade Segura TIPO 01 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 500MB.	Unidade	1589			
2	02.81.00.00192353-6	Solução de Conectividade Segura TIPO 02 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 2 links (redundância) de internet banda larga com velocidade de 500MB.	Unidade	707			

3	02.81.00.00192354-4	Solução de Conectividade Segura TIPO 03 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 1GB.	Unidade	109			
4	02.81.00.00192355-2	Solução de Conectividade Segura TIPO 04 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 2 links (redundância) de internet banda larga com velocidade de 1GB.	Unidade	167			
5	02.81.00.00192356-0	Solução de Conectividade Segura TIPO 05 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários em unidades remotas que não possuem viabilidade de conexão via fibra ótica, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 1 link satélite com velocidade de 100 MB.	Unidade	149			

6	02.81.00.00192357-9	Solução de Conectividade Segura TIPO 06 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 1 link de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.	Unidade	101			
7	02.81.00.00192358-7	Solução de Conectividade Segura TIPO 07 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 500MB.	Unidade	54			
8	02.81.00.00192359-5	Solução de Conectividade Segura TIPO 08 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 500MB.	Unidade	16			

9	02.81.00.00192360-9	Solução de Conectividade Segura TIPO 09 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 1GB.	Unidade	78			
10	02.81.00.00192361-7	Solução de Conectividade Segura TIPO 10 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 1GB.	Unidade	33			
11	02.81.00.00192362-5	Solução de Conectividade Segura TIPO 11 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB.	Unidade	91			
12	02.81.00.00192363-3	Solução de Conectividade Segura TIPO 12 Solução de conectividade segura prestada em regime	Unidade	14			

		contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB e 1 link de internet banda larga com velocidade de 500MB.					
13	02.81.00.00192364-1	Solução de Conectividade Segura TIPO 13 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades com até 40 usuários e que já possuem link de internet contemplando 01 firewall de próxima geração (NGFW) com tecnologia SD-WAN.	Unidade	105			
14	02.81.00.00192365-0	Solução de Conectividade Segura TIPO 14 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades acima de 40 usuários e que já possuem link de internet contemplando 01 firewall de próxima geração (NGFW) com tecnologia SD-WAN.	Unidade	50			
15	02.81.00.00192366-8	Solução de Conectividade Segura TIPO 15 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários,	Unidade	20			

		incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN, 2 links (redundância) de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.					
16	02.81.00.00192367-6	Solução de Conectividade Segura TIPO 16 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN, 2 links (redundância) de internet banda larga com velocidade de 1GB e 1 link satélite com velocidade de 100 MB.	Unidade	16			
17	02.81.00.00192368-4	Solução de Conectividade Segura TIPO 17 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, destinada a unidades com até 05 usuários, contemplando 1 link de internet banda larga com velocidade de 200 Mbps e mecanismos de segurança providos de forma centralizada, sob gestão da PRODEB, sem a necessidade de firewall de borda dedicado na unidade.	Unidade	369			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)	

18	02.81.00.00192370-6	Serviço de Mudança de Endereço – até 300 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	137			
19	02.81.00.00192371-4	Serviço de Mudança de Endereço – acima de 300 km até 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	144			
20	02.81.00.00192372-2	Serviço de Mudança de Endereço – acima de 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	108			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor mensal unitário (R\$) A	Valor unitário para 60 meses (R\$) B = A * 60	Valor Total 60 meses (R\$) C = B * QTD

21	02.81.09.00008168-0	Solução de Operação e Monitoramento Central, prestada em regime contínuo e remunerada por valor mensal, dimensionada para atender até 500 (quinhentas) unidades de solução de conectividade segura em operação	Unidade	10			
22	02.81.09.00008169-8	Solução de Monitoramento e Relatoria De Logs Tipo I	Unidade	02			
23	02.81.00.00192944-5	Solução de Monitoramento e Relatoria De Logs Tipo II	Unidade	50			
24	02.81.00.00192945-3	Solução de Monitoramento e Relatoria De Logs Tipo III	Unidade	04			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)		Valor Total (R\$)
25	02.81.00.00192946-1	UST – Unidade de Serviços Técnicos	Unidade	5.000			
Valor Global do Lote 01:							

LOTE 02						
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)
1	02.81.00.00192373-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600E, pelo período de 12 meses	Unidade	04		
2	02.81.00.00192374-9	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 601E, pelo período de 12 meses	Unidade	04		

3	02.81.00.00192375-7	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 400F, pelo período de 12 meses	Unidade	08		
4	02.81.00.00192376-5	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200F, pelo período de 12 meses	Unidade	09		
5	02.81.00.00192377-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200E, pelo período de 12 meses	Unidade	04		
6	02.81.00.00192378-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 100F, pelo período de 12 meses	Unidade	24		
7	02.81.00.00192379-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 80F, pelo período de 12 meses	Unidade	12		
8	02.81.00.00192380-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 60F, pelo período de 12 meses	Unidade	300		

9	02.81.00.00192381-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 61F, pelo período de 12 meses	Unidade	300		
10	02.81.00.00192382-0	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 150G, pelo período de 12 meses	Unidade	04		
11	02.81.00.00192383-8	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 300G, pelo período de 12 meses	Unidade	04		
12	02.81.00.00192384-6	Serviço de Licenciamento e Atualização das Funcionalidades de Autenticação Centralizada de Usuários Marca Fortinet Modelo FortiAuthenticator 800F, pelo período de 12 meses	Unidade	04		
13	02.81.00.00192385-4	Solução De Segurança de Rede NGFW TIPO I, com licenciamento pelo período de 12 meses	Unidade	04		
14	02.81.00.00192386-2	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede - Segmentação Interna TIPO I, pelo período de 12 meses	Unidade	04		

15	02.81.00.00192947-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3700F, pelo período de 12 meses	Unidade	04		
16	02.81.00.00192948-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3301E, pelo período de 12 meses	Unidade	04		
17	02.81.00.00192949-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3000D, pelo período de 12 meses	Unidade	02		
18	02.81.00.00192950-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600F, pelo período de 12 meses	Unidade	04		
19	02.81.00.00192951-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 40F, pelo período de 12 meses	Unidade	60		
20	02.81.00.00192952-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate-VM08, pelo período de 12 meses	Unidade	02		

21	02.81.00.00192953-4	Serviço de Licenciamento e Atualização das Funcionalidades de WAF Marca Fortinet Modelo FortiWeb2000F, pelo período de 12 meses	Unidade	04		
22	02.81.00.00192954-2	Serviço de Licenciamento e Atualização das Funcionalidades de ADC Marca Fortinet Modelo FortiADC-400F, pelo período de 12 meses	Unidade	02		
23	02.80.00.00192955-0	Serviço de Licenciamento e Atualização das Funcionalidades de Gerenciador Centralizada de Dispositivos Marca Fortinet Modelo FortiManager 3000G, pelo período de 12 meses	Unidade	02		
24	02.81.00.00192956-9	Serviço de Licenciamento e Atualização das Funcionalidades de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	02		
25	02.81.00.00192957-7	Serviço de Upgrade para 50 Devices e 500 EPS de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	04		
26	02.81.00.00192958-5	Solução De Segurança de Aplicações WAF - TIPO I, com licenciamento pelo período de 12 meses	Unidade	02		
27	02.81.00.00192959-3	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF - TIPO I, pelo período de 12 meses	Unidade	02		

28	02.81.00.00192989-5	Solução De Segurança de Aplicações WAF - TIPO II, com licenciamento pelo período de 12 meses	Unidade	10		
29	02.81.00.00192990-9	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF –TIPO II, pelo período de 12 meses	Unidade	10		
30	02.81.00.00192962-3	Solução de Segurança de Aplicações WAF para Ambientes Híbridos, com licenciamento pelo período de 12 meses	Unidade	10		
31	02.81.00.00192963-1	Serviço de Licenciamento e Atualização das Funcionalidades de Solução de Segurança de Aplicações WAF para Ambientes Híbridos, pelo período de 12 meses	Unidade	10		
32	02.81.00.00192964-0	Solução de Segurança Decoy/Honeypot, com licenciamento pelo período de 12 meses	Unidade	06		
33	02.81.00.00192965-8	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança Decoy/Honeypot, pelo período de 12 meses	Unidade	06		
34	02.81.00.00192966-6	Solução de Segurança de Rede NGFW TIPO II, com licenciamento pelo período de 12 meses	Unidade	100		
35	02.81.00.00192967-4	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna TIPO II, pelo período de 12 meses	Unidade	100		
36	02.81.00.00192968-2	Solução de Segurança de Rede NGFW TIPO III, com licenciamento pelo período de 12 meses	Unidade	50		
37	02.81.00.00192969-0	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna	Unidade	50		

		TIPO III, pelo período de 12 meses				
Valor Global do Lote 02						R\$

4.2 A proposta de preço da empresa arrematante consta como Anexo II da presente Ata de Registro de Preços.

5. DOTAÇÃO ORÇAMENTÁRIA

5.1 A indicação da disponibilidade de créditos orçamentários somente será exigida para a formalização do termo de contrato ou, nas hipóteses previstas no art. 164 do RLC/PRODEB e art. 95 da Lei Federal nº 14.133/2021, do instrumento hábil que lhe substitua (art. 11 do Decreto 23.657/2025).

5.2 As despesas decorrentes da contratação correrão à conta da dotação orçamentária concernente ao órgão ou entidade contratante, devendo cada contratação ser precedida da emissão da declaração de compatibilidade com a Previsão Orçamentária da PRODEB e com a Lei de Responsabilidade Fiscal – LRF, quando for o caso.

6. CONTRATAÇÃO

Diretrizes gerais

6.1 A contratação do fornecedor com preço registrado será formalizada pelo órgão ou pela entidade interessada por meio de termo de contrato ou, nas hipóteses previstas no art. 164 do RLC/PRODEB e no art. 95 da Lei Federal nº 14.133/2021, por instrumento hábil que lhe substitua: Autorização de Fornecimento de Material - AFM ou Autorização de Prestação de Serviços – APS, conforme o caso. (art. 44 do Decreto 23.657/2025)

6.1.1 A contratação obedecerá as estipulações constantes da minuta de contrato integrante do edital da licitação.

6.1.2 Na hipótese de substituição do termo de contrato por outro instrumento hábil, neste serão consideradas literalmente transcritas todas as cláusulas e condições previstas na minuta de contrato referida no subitem 6.1.1.

6.1.3 Os instrumentos de que trata o subitem 6.1 serão assinados no prazo de validade da ata de registro de preços.

6.1.4 Como requisito para a celebração do contrato, o fornecedor deverá manter todas as condições de habilitação exigidas na licitação.

6.1.5 A divulgação do contrato observará o disposto no art. 182, §1º do RLC/PRODEB e no art. 94 da Lei Federal nº 14.133/2021.

6.2. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o disposto no art. 175 do RLC/PRODEB e no art. 124 da Lei Federal nº 14.133/2021 (art. 45 do Decreto 23.657/2025).

6.3 A vigência das contratações decorrentes do sistema de registro de preços obedecerá o disposto no TR, observada a disciplina do RLC/PRODEB e da Lei Federal nº 14.133/2021 (art. 46 do Decreto 23.657/2025).

Convocação para assinatura do termo de contrato

6.4 O Fornecedor com preço registrado será convocado a assinar o termo de contrato, AFM ou APS, se for o caso, no prazo fixado no Preâmbulo do Edital, nos termos do art. 167 do RLC/PRODEB, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas no RLC/PRODEB, na Lei Federal nº 14.133/2021, e em outras legislações aplicáveis.

6.4.1 O prazo de convocação poderá ser prorrogado uma vez, por até igual período, mediante solicitação do Fornecedor durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

6.4.2 O termo de contrato, a AFM ou, a APS, conforme o caso, deverá ser assinado pelo representante legal do Fornecedor com preço registrado ou mandatário com poderes expressos.

6.4.3 A assinatura se dará por meio do Sistema Eletrônico de Informações - SEI, caso em que a Fornecedor deverá providenciar o cadastramento de seu representante legal ou procurador no endereço eletrônico www.portalseibahia.saeb.ba.gov.br ou através do link disponibilizado www.comprasnet.ba.gov.br.

Recusa

6.5 A recusa injustificada do Fornecedor com preço registrado em subscrever o termo de contrato, AFM ou APS, conforme o caso, ensejará a aplicação das penalidades legalmente estabelecidas.

6.5.1 Equipara-se à recusa prevista no subitem 6.5 a circunstância de o Fornecedor com preço registrado deixar de manter as condições de habilitação exigidas na licitação ou no procedimento de contratação direta, ou, por qualquer meio, dar causa à impossibilidade da contratação.

6.5.2 A recusa do fornecedor com preço registrado em se cadastrar ou subscrever eletronicamente o termo de contrato, AFM ou APS, conforme o caso, implicará na decadência da contratação e à sujeição às sanções cominadas na legislação.

6.6 Inviabilizada a contratação por responsabilidade do fornecedor, a Administração comunicará o fato ao órgão gerenciador para adoção das providências pertinentes.

7. MODIFICAÇÃO DOS PREÇOS REGISTRADOS

Hipóteses de modificação (art. 25 do Decreto 23.657/2025)

7.1 Os preços registrados em ata poderão ser modificados em decorrência das seguintes situações:

I – redução do preço praticado no mercado;

II – reajustamento ou repactuação; ou

III – fato superveniente que impossibilite o cumprimento do compromisso na forma pactuada.

7.1.1 A hipótese prevista no inciso III deste subitem compreenderá o caso de força maior, o caso fortuito, fato do príncipe ou as situações decorrentes de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata, nos termos do disposto no art. 146 do RLC/PRODEB e na alínea “d” do inciso II do *caput* do art. 124 da Lei Federal nº 14.133/2021.

7.1.2 Inclui-se na previsão do inciso III deste subitem, ainda, a criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços registrados.

7.1.3 A modificação dos preços registrados em ata não implica a modificação automática dos preços dos contratos decorrentes do respectivo registro de preços.

Redução do preço praticado no mercado (art. 26 do Decreto 23.657/2025)

7.2 Na hipótese de o preço registrado tornar-se, por motivo superveniente, desvantajoso, em razão da redução do preço praticado no mercado, ou quando houver diminuição, devidamente comprovada, dos preços dos insumos básicos utilizados, o órgão ou a entidade gerenciadora convocará o fornecedor para negociar a adequação do preço registrado.

7.2.1 O fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidade, se não aceitar reduzir seu preço, caso em que será procedido ao cancelamento do preço registrado.

7.2.2 Na hipótese prevista no 7.2.1 deste subitem, o órgão ou a entidade gerenciadora poderá convocar os integrantes do cadastro de reserva, para verificar se aceitam reduzir seus preços.

7.2.3 Havendo mais de um interessado na redução do preço, prevalecerá a proposta de menor preço e, como critério de desempate, a precedência do licitante na ordem de classificação do cadastro de reserva.

7.2.4 Não havendo possibilidade de redução do preço, o órgão ou a entidade gerenciadora procederá ao cancelamento do item registrado, conforme o subitem 8.3 desta ata.

7.2.5 Na hipótese de redução do preço registrado, o órgão ou a entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços, para que avaliem a conveniência e a oportunidade de diligenciar negociação com vistas à alteração dos respectivos contratos.

Reajustamento e repactuação dos preços registrados (art. 27 do Decreto 23.657/2025)

7.3 O reajustamento e a repactuação dos preços registrados observarão os mesmos critérios definidos para o reajustamento e a repactuação do contrato.

7.3.1 Precedentemente ao reajustamento ou à repactuação do preço registrado, o órgão ou a entidade gerenciadora poderá identificar, entre os preços constantes do cadastro de reserva, aquele que possibilite a manutenção do mesmo preço registrado ou a obtenção de preço mais vantajoso que o resultante do cálculo realizado, desde que não seja superior ao preço originariamente ofertado pelo próprio licitante integrante da reserva.

7.3.2 Inexitosa a providência de que trata o subitem 7.3.1, o órgão ou a entidade gerenciadora procederá ao reajustamento ou à repactuação do preço registrado ou, mediante justificativa, à liberação do fornecedor do compromisso assumido quanto ao item registrado, sem aplicação de penalidade, procedendo ao cancelamento do preço e do item registrado, conforme o subitem 8.3 desta ata.

Fato superveniente que impossibilite o cumprimento do compromisso na forma pactuada (art. 28 do Decreto 23.657/2025)

7.4 Na hipótese de o preço de mercado se tornar superior ao preço registrado, inviabilizando o atendimento das obrigações estabelecidas em ata, será facultado ao fornecedor requerer ao órgão ou à entidade gerenciadora a alteração

do preço registrado, mediante comprovação do fato superveniente que o impossibilite de cumprir o compromisso na forma pactuada.

7.4.1 Para fins do disposto no subitem 7.4, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória e a planilha de custos que demonstre a inviabilidade da manutenção do preço registrado em relação às condições inicialmente pactuadas.

7.4.2 A impossibilidade do cumprimento da obrigação na forma como pactuada, ainda que temporária, deverá ser comunicada pelo fornecedor antes do pedido de fornecimento, e o preço registrado ficará suspenso até a decisão final da Administração.

7.4.3 Na hipótese de caso fortuito ou força maior que impossibilite definitivamente a execução da obrigação, o fornecedor poderá requerer, de logo, a liberação do compromisso assumido, apresentando os motivos e alegações que fundamentem a sua ocorrência, os quais, se confirmados, ensejarão o cancelamento do preço registrado, sem aplicação de penalidade.

7.4.4 A autoridade a quem competir a apreciação do requerimento deverá emitir a sua decisão motivada no prazo de 30 (trinta) dias, contado da data em que receber os autos conclusos, o qual poderá ser prorrogado por igual período, mediante motivação expressa.

7.4.5 Não sendo comprovada a existência de fato superveniente que inviabilize o cumprimento do compromisso, o pedido será indeferido e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do preço registrado, sem prejuízo da aplicação das sanções previstas no RLC/PRODEB, na Lei Federal nº 14.133/2021, na Lei nº 14.634/2023, e na legislação aplicável.

7.5 Comprovado o fato superveniente ensejador da alteração do preço registrado e procedida à aferição da planilha de custos que instruiu o pedido, o órgão ou a entidade gerenciadora procederá ao cálculo do novo preço. (art. 29 do Decreto 23.657/2025)

7.5.1 Para fins do subitem 7.5, em nenhuma hipótese, serão admitidos preços incompatíveis com os preços praticados no mercado ou fixados pela PRODEB ou por órgão oficial competente ou constantes de tabela de preços referenciais.

7.5.2 Precedentemente à alteração do preço registrado, o órgão ou a entidade gerenciadora poderá identificar, entre os preços constantes do cadastro de reserva, aquele que possibilite a manutenção do mesmo preço registrado ou a obtenção de preço mais vantajoso que o resultante do cálculo realizado, desde que não seja superior ao preço originariamente ofertado pelo próprio licitante integrante da reserva.

7.5.3 Inexistente a providência do subitem 7.5.1, o órgão ou a entidade gerenciadora procederá à alteração do preço registrado ou, mediante justificativa, à liberação do fornecedor do compromisso assumido quanto ao item registrado, sem aplicação de penalidade, procedendo ao cancelamento do preço e do item registrado, conforme o subitem 8.3 desta ata.

8. CANCELAMENTO DO PREÇO E DO ITEM REGISTRADO

Cancelamento do preço registrado (art. 30 do Decreto 23.657/2025)

8.1 O cancelamento dos preços registrados poderá ser realizado, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

I – quando o fornecedor estiver liberado do compromisso assumido quanto ao item registrado, nas hipóteses previstas nesta ata;

II – na hipótese do subitem 7.4.5 desta ata, em caso de recusa do fornecedor com preço registrado ao cumprimento das obrigações estabelecidas na ata, após o indeferimento do pedido de alteração do preço;

III – como efeito da imposição de sanção restritiva de direito irrecorrível, por infração administrativa prevista na Lei Federal nº 14.133/2021, e na Lei nº 14.634/2023, aplicada em processo administrativo sancionatório, nos termos do Decreto nº 23.113/2024;

IV – por razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade gerenciadora, formalmente motivadas nos autos do processo, assegurados o contraditório e a ampla defesa;

V- demais hipóteses previstas no art. 144 do RLC/PRODEB.

8.1.1 Será admitida a suspensão provisória de preço registrado, em caráter cautelar, no caso de risco iminente da ocorrência de fato que possa trazer prejuízo ao erário ou lesão ao interesse público de difícil ou impossível reparação.

8.1.2 O cancelamento do preço registrado será formalizado por ato do órgão ou da entidade gerenciadora.

Acionamento do cadastro de reserva em razão do cancelamento do preço registrado

8.2 Ressalvada a existência de previsão específica nesta ata, na hipótese de cancelamento do preço registrado, havendo possibilidade de substituição do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os integrantes do cadastro de reserva, na forma do subitem 5.2 da **Seção II, Parte III - do Sistema do Registro de Preços do Edital**, observada a ordem de classificação (art. 31 do Decreto 23.657/2025).

Cancelamento do item registrado

8.3 Cancelado o preço registrado e não havendo possibilidade de substituição do respectivo fornecedor por integrante do cadastro de reserva, será procedido ao cancelamento do item registrado (art. 32 do Decreto 23.657/2025).

Da substituição de marca (art. 33 do Decreto 23.657/2025)

8.4 Alternativamente ao cancelamento do item registrado, poderá ser admitida a substituição da marca do produto por outro de qualidade equivalente ou superior à registrada, vedada a fixação de valor superior ao anteriormente registrado.

8.4.1. A substituição da marca será precedida de parecer técnico fundamentado, no qual seja demonstrado o atendimento das especificações e dos requisitos pertinentes ao objeto, bem como a adequação do preço e dependerá de autorização da autoridade competente.

9. GERENCIAMENTO DOS QUANTITATIVOS DA ATA DE REGISTRO DE PREÇOS

Vedação ao acréscimo quantitativo da Ata

9.1 É vedado acréscimo ao quantitativo fixados na ata de registro de preços, sendo permitidos acréscimos apenas nos contratos dela decorrentes, nos termos do art. 137, §2º do RLC/PRODEB.

Remanejamento de quantitativos (art. 35 do Decreto 23.657/2025)

9.2 Ressalvada a existência de disposição diversa no TR, as quantidades previstas para os itens com preços registrados na ata de registro de preços poderão ser remanejadas pelo órgão ou pela entidade gerenciadora entre os órgãos ou entidades participantes.

9.2.1 O órgão ou a entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para fins do remanejamento de que trata o subitem 9.2.

9.2.2 Competirá ao órgão ou à entidade gerenciadora autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pelo órgão ou pela entidade participante, desde que haja prévia anuência do órgão ou da entidade que sofrer redução dos quantitativos informados.

9.2.3 Fica vedado o remanejamento de quantitativos, enquanto houver disponibilidade de contratação dos itens registrados para o órgão ou entidade solicitante.

10. COMPARTILHAMENTO, POR ADESÃO, DA ATA DE REGISTRO DE PREÇOS

Requisitos da admissão à adesão (art. 40 do Decreto 23.657/2025)

10.1 A PRODEB poderá admitir a adesão de órgãos ou entidades não participantes a esta ata de registro de preços, desde que previamente autorizada pelo órgão gerenciador e **condicionada à análise e manifestação favorável da Secretaria da Administração do Estado da Bahia – SAEB.**

10.1.1 PRODEB poderá admitir, na qualidade de não participante, a adesão de órgão ou entidade estadual a ata de registro de preços para aqueles itens para os quais não tenha quantitativo registrado, observados os requisitos previstos neste item 10.1

10.1.2 A análise da juridicidade da participação, da inexistência de norma interna impeditiva, bem assim da adequação e compatibilidade com o regime jurídico de licitação a que está submetido o órgão ou a entidade gerenciadora, deverá ser procedida pelo órgão ou entidade que pretende a adesão.

10.1.3 A juridicidade da inclusão a que se refere o subitem 10.1.2 é presumida, quando submetidos os órgãos e entidades ao mesmo regime jurídico geral de licitações e contratos, sem prejuízo da avaliação da compatibilidade das especificidades decorrentes da legislação suplementar e normas regulamentares incidentes.

Limite quantitativo da adesão (art. 41 do Decreto 23.657/2025)

10.2 Serão observadas as seguintes regras de controle para a adesão a esta ata de registro de preços:

I - as contratações adicionais não poderão exceder, por órgão ou entidade solicitante, a 50% (cinquenta por cento) dos quantitativos dos itens registrados na ata de registro de preços para a PRODEB e para os órgãos ou as entidades participantes; e

II - o quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para a PRODEB e os órgãos ou as entidades participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

Procedimento da adesão

10.3 No procedimento de adesão de órgão ou entidade não participante a ata de registro de preços, os órgãos e entidades interessados deverão consultar a PRODEB para manifestação sobre a possibilidade de adesão, **condicionada à análise**

e manifestação favorável da Secretaria da Administração do Estado da Bahia – SAEB. (art. 42 do Decreto 23.657/2025).

10.3.1 Caberá ao fornecedor da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação, ou não, do fornecimento decorrente de adesão.

10.3.2 A autorização da PRODEB apenas será realizada após a aceitação da adesão pelo fornecedor.

10.3.3 Após a autorização da PRODEB, o órgão ou a entidade não participante efetivará a contratação no prazo que lhe for assinalado, desde que respeitado o limite temporal de vigência da ata de registro de preços.

Obrigações decorrentes da adesão

10.4 Compete ao órgão ou à entidade aderente à ata de registro de preços estadual (art. 7º, incisos V a VII, e art. 43 do Decreto 23.657/2025):

I - observar as disposições da ata de registro de preços e de suas eventuais alterações, para o seu correto cumprimento;

II – acompanhar a execução de suas contratações, procedendo:

a) à cobrança do cumprimento, pelo fornecedor, das obrigações contratualmente assumidas;

b) à adoção, observadas as disposições legais pertinentes, das providências necessárias à apuração de ilícitos verificados, aplicando as sanções administrativas de sua competência;

c) à comunicação a PRODEB das ocorrências que possam impactar no cumprimento da ata de registro de preços;

III - prestar as informações solicitadas pela PRODEB quanto às suas contratações;

IV – atender às obrigações que lhe forem assinaladas pela PRODEB.

11. SANÇÕES ADMINISTRATIVAS

11.1 O descumprimento da Ata de Registro de Preços ensejará a aplicação das sanções administrativas referidas no RLC/PRODEB, na Lei nº 14.634/2023, no Decreto Estadual nº 23.113/2024, no Decreto Estadual nº 24.318/2026 e às demais cominações legais, resguardado o direito à ampla defesa e ao contraditório.

12. COMUNICAÇÃO ELETRÔNICA

12.1. Fica pactuado que os atos de comunicação processual com o Fornecedor detentor da ata poderão ser realizados por meio eletrônico, na forma do disposto na Lei nº 12.209, de 20 de abril de 2011, e do Decreto nº 15.805, de 30 de dezembro de 2014.

12.1.1. O Fornecedor deverá manter atualizado o endereço eletrônico cadastrado no Sistema Eletrônico de Informações - SEI, para efeito do recebimento de notificação e intimação de atos processuais, conforme Decreto estadual nº 17.983, de 24 de outubro de 2017, devendo atender às convocações da PRODEB para a prática de atos nos prazos indicados.

13. DISPOSIÇÕES FINAIS

13.1 Integram a presente Ata, como se nela estivessem transcritas, todas as cláusulas e condições estabelecidas na licitação, inclusive anexos, apêndices e adendos, e a proposta do Fornecedor.

14. FORO

14.1 As partes elegem o Foro da Cidade do Salvador, Estado da Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para solucionar quaisquer dúvidas oriundas deste instrumento que não puderem ser dirimidas por quaisquer dos meios alternativos de resolução de controvérsias de que trata o RLC/PRODEB, a Lei Federal nº 14.133/2021 e a Lei nº 14.783/2024.

Salvador, ____ de _____ de 2026.

Pela **CONTRATANTE/PRODEB**:

José Muniz Rebouças
Diretor Executivo

Carlos Augusto Borges Silva
Diretor de Infraestrutura Tecnológica e Conectividade

Pela **CONTRATADA**:

Nome Representante: XXXXX
Fornecedor: XXXXX

ANEXO I

CADASTRO RESERVA

- 1. Seguindo a ordem de classificação, segue relação de fornecedores que aceitaram cotar os itens com preços iguais aos do adjudicatário:**
- 2. Seguindo a ordem de classificação, segue relação de fornecedores que mantiveram sua proposta original:**

ANEXO II

PROPOSTA DE PREÇOS DO FORNECEDOR

ANEXO III – MINUTAS DE CONTRATOS

MINUTA PRODEB

CONTRATO Nº/.....-....

A COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DA BAHIA-PRODEB, sociedade de economia mista, com sede nesta Capital na Avenida Quatro, Nº 410 - Centro Administrativo da Bahia, inscrita no CNPJ sob o Nº 13.579.586/0001-32, neste ato representada pelos seus Diretores Executivo e de Infraestrutura Tecnológica e Conectividade, respectivamente, Srs. José Muniz Rebouças e Carlos Augusto Borges Silva, doravante denominada simplesmente **PRODEB**, e a (o), com sede na Rua, nº, ..., ..., ..., inscrita no CNPJ sob Nº, legalmente representada pelo seu....., Sr., portador da carteira de identidade nº, expedida pela e do CPF nº, residente e domiciliado na, Estado da, tendo como responsável(eis) técnico(s) o(s) Sr.(s), ..., portador(es) da(s) carteira(s) de identidade nº(s), CPF nº(s), doravante denominada simplesmente **CONTRATADA** com respaldo no rito similar ao Pregão Eletrônico nº 005/2026 de que trata o Processo Administrativo SEI nº 065.10933.2026.0003946-61, celebram o presente contrato, que se regerá pela Lei Federal nº 13.303/2016 e pelo Regulamento de Licitações e Contratos - RLC da PRODEB, aprovado pelo CAD em 29/06/2018, alterado em 18/06/2024 e subsidiariamente, pelas Leis nºs 14.133/2021 e 14.634/2023, bem como pela Lei Complementar nº 123/2006 e suas alterações, da Lei Federal nº 13.709/2018, do Decreto Estadual nº 22.886/2024, do Decreto Estadual nº 22.888/2024, do Decreto Estadual nº 23.113/2024, do Decreto Estadual nº 23.356/2025, do Decreto Estadual nº 23.657/2025, do Decreto Estadual nº 24.318/2026 e respectivas alterações e demais legislações pertinentes, mediante as cláusulas e condições a seguir ajustadas:

CLÁUSULA PRIMEIRA – FUNDAMENTO LEGAL

O presente ajuste, na forma da fundamentação legal indicada no preâmbulo, decorre do Pregão Eletrônico nº 005/2026, devidamente homologado em/...../..... pela Diretoria Executiva da CONTRATANTE (DOC. SEI.....) e da Ata de Registro de Preços nº/....., tudo constante do Processo Administrativo SEI nº 065.10933.2026.0003946-61, que fica fazendo parte integrante do presente contrato, regendo-o no que for omissivo.

CLÁUSULA SEGUNDA - OBJETO

Constitui objeto do presente instrumento a contratação dos serviços/fornecimento especificados no **Lote 1/Lote 2** do Termo de Referência que constitui o ANEXO I, de acordo com as especificações e obrigações consignadas na Requisição de Compras nº, com as demais condições previstas neste contrato e na Proposta de Preços apresentada pela CONTRATADA que constitui o ANEXO II.

§1º O objeto deste contrato deverá ser executado de acordo com o Termo de Referência (DOC. SEI 00139550606), parte integrante deste Contrato.

§2º PARA O LOTE 1: Em havendo subcontratação a CONTRATADA deverá submeter à apreciação da CONTRATANTE a proposta de subcontratação, com descrição dos serviços e comprovação do respectivo limite fixado no Edital e no item 16.1 a 16.9 do Termo de Referência, bem como do atendimento da qualificação técnica conforme exigido no § 3º, do art. 171 do RLC/PRODEB.

§2º PARA O LOTE 2: É vedada a subcontratação do objeto, a associação da CONTRATADA com outrem, a cessão ou transferência, total ou parcial do contrato, bem como a fusão, cisão ou incorporação da CONTRATADA, não se responsabilizando a CONTRATANTE por nenhum compromisso assumido por aquela

com terceiros, sob pena da incidência das consequências previstas neste instrumento, nos termos do item 16.10 do Termo de Referência.

§3º O objeto deste contrato não pode sofrer solução de continuidade durante todo o prazo da sua vigência, devendo ser executado por empregados/prepostos da CONTRATADA, sob a inteira responsabilidade funcional, operacional, mediante estrito e exclusivo controle desta.

CLÁUSULA TERCEIRA - PRAZO

PARA O LOTE 1: O prazo de vigência do contrato a contar da data da sua assinatura, será de 05 (cinco) anos, ficando a sua eficácia condicionada à publicação do extrato na imprensa oficial, não sendo passível de renovação, nos termos e condições do art. 71 da Lei nº 13.303/2016, com correspondência no artigo 160 do RLC/PRODEB, e demais normas concernentes à matéria, **conforme previsto no item 21.1.2 do Termo de Referência.**

PARA O LOTE 2: O prazo de vigência do contrato a contar da data da sua assinatura, será de 12 (doze) meses, ficando a sua eficácia condicionada à publicação do extrato na imprensa oficial, admitindo-se a sua prorrogação, nos termos e condições do art. 71 da Lei nº 13.303/2016, com correspondência no artigo 160 do RLC/PRODEB, e demais normas concernentes à matéria, **conforme previsto no item 21.2 do Termo de Referência.**

PARA O LOTE 2:

§1º A prorrogação do prazo de vigência está condicionada à obtenção de preços e condições mais vantajosas.

§2º A prorrogação deverá ser previamente justificada e autorizada pela autoridade competente para celebrar o ajuste e será realizada através de termo aditivo, devendo o pedido ser realizado no prazo máximo de 90 (noventa) dias antes do termo final do contrato, conforme prescreve o art. 183, Parágrafo único do Regulamento de Licitações e Contratos - RLC da PRODEB.

PARA AMBOS OS LOTES:

§3º O prazo de que trata o caput desta cláusula, poderá ser suspenso, caso ocorra as situações adiante relacionadas:

- a) paralisação da execução do objeto determinada pela CONTRATANTE, por motivo não imputável à CONTRATADA;
- b) motivo de força maior.

CLÁUSULA QUARTA – PREÇO

A **CONTRATANTE** pagará à **CONTRATADA**, pelos serviços/fornecimento descritos na **CLÁUSULA SEGUNDA** do presente instrumento, os valores devidos conforme proposta da CONTRATADA datada de ____/____/____, acostada ao Processo Administrativo SEI nº 065.10933.2026.0003946-61, passando a integrar o ANEXO II deste instrumento, possuindo o presente contrato o valor global de R\$ (.....):

LOTE 01							
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor mensal unitário (R\$) A	Valor unitário para 60 meses (R\$) B = A * 60	Valor Total 60 meses (R\$) C = B * QTD
1	02.81.00.00192352-8	Solução de Conectividade Segura TIPO 01 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 500MB.	Unidade	1589			
2	02.81.00.00192353-6	Solução de Conectividade Segura TIPO 02 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 2 links (redundância) de internet banda larga com velocidade de 500MB.	Unidade	707			
3	02.81.00.00192354-4	Solução de Conectividade Segura TIPO 03 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda	Unidade	109			

		larga com velocidade de 1GB.					
4	02.81.00.00192355-2	Solução de Conectividade Segura TIPO 04 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 2 links (redundância) de internet banda larga com velocidade de 1GB.	Unidade	167			
5	02.81.00.00192356-0	Solução de Conectividade Segura TIPO 05 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários em unidades remotas que não possuem viabilidade de conexão via fibra ótica, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 1 link satélite com velocidade de 100 MB.	Unidade	149			

6	02.81.00.00192357-9	Solução de Conectividade Segura TIPO 06 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 1 link de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.	Unidade	101			
7	02.81.00.00192358-7	Solução de Conectividade Segura TIPO 07 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 500MB.	Unidade	54			
8	02.81.00.00192359-5	Solução de Conectividade Segura TIPO 08 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 500MB.	Unidade	16			

9	02.81.00.00192360-9	Solução de Conectividade Segura TIPO 09 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 1GB.	Unidade	78			
10	02.81.00.00192361-7	Solução de Conectividade Segura TIPO 10 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 1GB.	Unidade	33			
11	02.81.00.00192362-5	Solução de Conectividade Segura TIPO 11 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB.	Unidade	91			
12	02.81.00.00192363-3	Solução de Conectividade Segura TIPO 12 Solução de conectividade segura prestada em regime	Unidade	14			

		contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB e 1 link de internet banda larga com velocidade de 500MB.					
13	02.81.00.00192364-1	Solução de Conectividade Segura TIPO 13 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades com até 40 usuários e que já possuem link de internet contemplando 01 firewall de próxima geração (NGFW) com tecnologia SD-WAN.	Unidade	105			
14	02.81.00.00192365-0	Solução de Conectividade Segura TIPO 14 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades acima de 40 usuários e que já possuem link de internet contemplando 01 firewall de próxima geração (NGFW) com tecnologia SD-WAN.	Unidade	50			
15	02.81.00.00192366-8	Solução de Conectividade Segura TIPO 15 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários,	Unidade	20			

		incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN, 2 links (redundância) de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.					
16	02.81.00.00192367-6	Solução de Conectividade Segura TIPO 16 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN, 2 links (redundância) de internet banda larga com velocidade de 1GB e 1 link satélite com velocidade de 100 MB.	Unidade	16			
17	02.81.00.00192368-4	Solução de Conectividade Segura TIPO 17 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, destinada a unidades com até 05 usuários, contemplando 1 link de internet banda larga com velocidade de 200 Mbps e mecanismos de segurança providos de forma centralizada, sob gestão da PRODEB, sem a necessidade de firewall de borda dedicado na unidade.	Unidade	369			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)	

18	02.81.00.00192370-6	Serviço de Mudança de Endereço – até 300 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	137			
19	02.81.00.00192371-4	Serviço de Mudança de Endereço – acima de 300 km até 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	144			
20	02.81.00.00192372-2	Serviço de Mudança de Endereço – acima de 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	108			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor mensal unitário (R\$) A	Valor unitário para 60 meses (R\$) B = A * 60	Valor Total 60 meses (R\$) C = B * QTD

21	02.81.09.00008168-0	Solução de Operação e Monitoramento Central, prestada em regime contínuo e remunerada por valor mensal, dimensionada para atender até 500 (quinhentas) unidades de solução de conectividade segura em operação	Unidade	10			
22	02.81.09.00008169-8	Solução de Monitoramento e Relatoria De Logs Tipo I	Unidade	02			
23	02.81.00.00192944-5	Solução de Monitoramento e Relatoria De Logs Tipo II	Unidade	50			
24	02.81.00.00192945-3	Solução de Monitoramento e Relatoria De Logs Tipo III	Unidade	04			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)		Valor Total (R\$)
25	02.81.00.00192946-1	UST – Unidade de Serviços Técnicos	Unidade	5.000			
Valor Global do Lote 01:							

LOTE 02						
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)
1	02.81.00.00192373-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600E, pelo período de 12 meses	Unidade	04		
2	02.81.00.00192374-9	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 601E, pelo período de 12 meses	Unidade	04		

3	02.81.00.00192375-7	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 400F, pelo período de 12 meses	Unidade	08		
4	02.81.00.00192376-5	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200F, pelo período de 12 meses	Unidade	09		
5	02.81.00.00192377-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200E, pelo período de 12 meses	Unidade	04		
6	02.81.00.00192378-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 100F, pelo período de 12 meses	Unidade	24		
7	02.81.00.00192379-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 80F, pelo período de 12 meses	Unidade	12		
8	02.81.00.00192380-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 60F, pelo período de 12 meses	Unidade	300		

9	02.81.00.00192381-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 61F, pelo período de 12 meses	Unidade	300		
10	02.81.00.00192382-0	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 150G, pelo período de 12 meses	Unidade	04		
11	02.81.00.00192383-8	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 300G, pelo período de 12 meses	Unidade	04		
12	02.81.00.00192384-6	Serviço de Licenciamento e Atualização das Funcionalidades de Autenticação Centralizada de Usuários Marca Fortinet Modelo FortiAuthenticator 800F, pelo período de 12 meses	Unidade	04		
13	02.81.00.00192385-4	Solução De Segurança de Rede NGFW TIPO I, com licenciamento pelo período de 12 meses	Unidade	04		
14	02.81.00.00192386-2	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede - Segmentação Interna TIPO I, pelo período de 12 meses	Unidade	04		

15	02.81.00.00192947-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3700F, pelo período de 12 meses	Unidade	04		
16	02.81.00.00192948-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3301E, pelo período de 12 meses	Unidade	04		
17	02.81.00.00192949-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3000D, pelo período de 12 meses	Unidade	02		
18	02.81.00.00192950-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600F, pelo período de 12 meses	Unidade	04		
19	02.81.00.00192951-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 40F, pelo período de 12 meses	Unidade	60		
20	02.81.00.00192952-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate-VM08, pelo período de 12 meses	Unidade	02		

21	02.81.00.00192953-4	Serviço de Licenciamento e Atualização das Funcionalidades de WAF Marca Fortinet Modelo FortiWeb2000F, pelo período de 12 meses	Unidade	04		
22	02.81.00.00192954-2	Serviço de Licenciamento e Atualização das Funcionalidades de ADC Marca Fortinet Modelo FortiADC-400F, pelo período de 12 meses	Unidade	02		
23	02.80.00.00192955-0	Serviço de Licenciamento e Atualização das Funcionalidades de Gerenciador Centralizada de Dispositivos Marca Fortinet Modelo FortiManager 3000G, pelo período de 12 meses	Unidade	02		
24	02.81.00.00192956-9	Serviço de Licenciamento e Atualização das Funcionalidades de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	02		
25	02.81.00.00192957-7	Serviço de Upgrade para 50 Devices e 500 EPS de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	04		
26	02.81.00.00192958-5	Solução De Segurança de Aplicações WAF - TIPO I, com licenciamento pelo período de 12 meses	Unidade	02		
27	02.81.00.00192959-3	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF - TIPO I, pelo período de 12 meses	Unidade	02		

28	02.81.00.00192989-5	Solução De Segurança de Aplicações WAF - TIPO II, com licenciamento pelo período de 12 meses	Unidade	10		
29	02.81.00.00192990-9	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF –TIPO II, pelo período de 12 meses	Unidade	10		
30	02.81.00.00192962-3	Solução de Segurança de Aplicações WAF para Ambientes Híbridos, com licenciamento pelo período de 12 meses	Unidade	10		
31	02.81.00.00192963-1	Serviço de Licenciamento e Atualização das Funcionalidades de Solução de Segurança de Aplicações WAF para Ambientes Híbridos, pelo período de 12 meses	Unidade	10		
32	02.81.00.00192964-0	Solução de Segurança Decoy/Honeypot, com licenciamento pelo período de 12 meses	Unidade	06		
33	02.81.00.00192965-8	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança Decoy/Honeypot, pelo período de 12 meses	Unidade	06		
34	02.81.00.00192966-6	Solução de Segurança de Rede NGFW TIPO II, com licenciamento pelo período de 12 meses	Unidade	100		
35	02.81.00.00192967-4	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna TIPO II, pelo período de 12 meses	Unidade	100		
36	02.81.00.00192968-2	Solução de Segurança de Rede NGFW TIPO III, com licenciamento pelo período de 12 meses	Unidade	50		
37	02.81.00.00192969-0	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna	Unidade	50		

		TIPO III, pelo período de 12 meses				
Valor Global do Lote 02						R\$

Parágrafo Único - Nos preços contratados estão incluídos todos os custos com material de consumo, salários, encargos sociais, previdenciários e trabalhistas de todo o pessoal da CONTRATADA, como também fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela CONTRATADA das obrigações, não cabendo quaisquer reivindicações desta à título de revisão de preço ou reembolso, seja a que título for, salvo àquelas presentes no § 4º do art. 81 da Lei nº 13.303/2016.

CLÁUSULA QUINTA - DOTAÇÃO ORÇAMENTÁRIA

As despesas para o pagamento deste contrato correrão por conta dos recursos da **CONTRATANTE**, conforme detalhado a seguir:

CENTRO DE CUSTO	FONTE	CONTA ORÇAMENTÁRIA

CLÁUSULA SEXTA - PAGAMENTO

Em consonância com o **§1º do art. 203** do Regulamento de Licitações e Contratos – RLC da PRODEB, os pagamentos devidos à CONTRATADA serão efetuados através de ordem bancária ou crédito em conta corrente, observada a ordem cronológica de apresentação das faturas aptas ao pagamento, **nas condições estabelecidas no item 18 do Termo de Referência**, e nos prazos adiante relacionados, contados da apresentação da fatura:

- até R\$ 50.000,00 o pagamento será efetuado em até 15 (quinze) dias;
- de R\$ 50.000,01 a R\$ 100.000,00 o pagamento será efetuado em até 30 (trinta) dias;
- acima de R\$ 100.000,01 o pagamento será efetuado em até 45 (quarenta e cinco) dias.

§1º A(s) nota(s) fisca(l)is/fatura(s) somente deverá(ao) ser apresentada(s) para pagamento após a conclusão da etapa do recebimento definitivo, atestada pelo Gestor e Fiscal do contrato, indicativo da satisfação pela CONTRATADA de todas as obrigações pertinentes ao objeto contratado, acompanhadas no que couber dos documentos abaixo relacionados:

- prova de regularidade relativa à Seguridade Social (INSS) e ao Fundo de Garantia por Tempo de Serviço (FGTS);
 - prova de Regularidade com a Fazenda Federal (Dívida Ativa da União e Receita Federal), Estadual e Municipal do domicílio da CONTRATADA;
- b.1. As empresas sediadas fora do Território da Bahia deverão apresentar, com a certidão de regularidade do seu Estado de origem, a certidão de regularidade para com a Fazenda Pública do Estado da Bahia.
- prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação da Certidão Negativa de Débitos Trabalhistas (CNDT);
 - certidão de regularidade com a Fazenda Pública Municipal (referente ao ISS) do(s) município(s) onde as obras ou serviços venham a ser prestados ou executados;

- e) guia de recolhimento do ISS quitada relativa à fatura, devidamente homologada pela Secretaria de Finanças do(s) município(s) onde se realizará a obra ou serviços, exceto para o município de Salvador;

- e.1. A guia de que trata esta alínea deverá identificar o número da Nota Fiscal a que o recolhimento se refere;
- e.2. Os municípios onde os serviços/obras são executados deverão ser informados na Nota Fiscal, bem como o percentual do serviço/obra executado em cada um, de acordo com relatório emitido pelo Fiscal do serviço/obra;
- e.3. A retenção e o recolhimento do ISS para o município de Salvador, caso haja, serão realizados pela CONTRATANTE.

§2º Ainda que a nota fiscal/fatura seja apresentada antes do prazo definido para recebimento definitivo, o prazo para pagamento somente fluirá após o efetivo atesto do recebimento definitivo.

§3º A CONTRATANTE descontará da fatura mensal o valor correspondente às faltas ou atrasos no cumprimento da obrigação, com base no valor do preço vigente, e ainda de eventuais multas conforme previsto no § 7º, da Cláusula Décima Terceira deste instrumento.

§4º A(s) nota(s) fiscal(is)/fatura(s) deverá(o) estar acompanhadas da documentação probatória pertinente, relativa ao recolhimento dos impostos relacionados com a obrigação.

§5º Em havendo alguma pendência impeditiva do pagamento, a exemplo de erro na apresentação da nota fiscal/fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como obrigações financeiras pendentes, decorrentes de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

§6º As situações previstas na legislação específica sujeitar-se-ão à emissão de nota fiscal eletrônica ou o respectivo DANFE (Documento Auxiliar de Nota Fiscal Eletrônica).

§7º A CONTRATANTE não receberá qualquer objeto da contratação que não esteja acompanhada do respectivo documento fiscal, na sua forma eletrônica, ou do respectivo DANFE (Documento Auxiliar de Nota Fiscal Eletrônica) e de todos os documentos necessários a instrução do pagamento, previstos neste instrumento.

§8º Caso a CONTRATADA seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, deverá apresentar, juntamente com a nota fiscal, a devida comprovação, a fim de evitar a retenção na fonte, dos tributos e contribuições, conforme legislação em vigor.

§9º É responsabilidade da CONTRATADA o pagamento de todos os tributos que, direta ou indiretamente, incidam sobre o objeto deste contrato, inclusive emolumentos e seguros, ficando excluída qualquer solidariedade da CONTRATANTE por eventuais autuações administrativas e/ou judiciais, uma vez que a inadimplência da CONTRATADA não se transfere à CONTRATANTE.

§10º A CONTRATANTE, quando fonte retentora, descontará e recolherá, nos prazos da Lei, dos pagamentos que efetuar, os tributos que seja obrigada a reter, conforme legislação vigente.

§11º A CONTRATADA deverá cumprir todas as Normas Regulamentadoras do Ministério do Trabalho, sem ônus para a CONTRATANTE.

§12º A atualização monetária dos pagamentos devidos pela CONTRATANTE, em caso de mora, será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE *pro rata tempore*.

CLÁUSULA SÉTIMA – GARANTIA

A garantia contratual será de 5% (cinco por cento) do valor do contrato, podendo recair sobre qualquer das modalidades previstas no § 1º do artigo 158, do Regulamento de Licitações e Contratos – RLC da PRODEB.

§1º Sob pena da caracterização de inadimplemento contratual, a prova da garantia, deverá ser apresentada no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério da CONTRATANTE, contados da data da assinatura deste contrato, sem o que fica vedada, em qualquer caso, a realização do pagamento.

§2º A garantia responderá pelo inadimplemento das obrigações contratuais e pelas multas impostas, independentemente de outras cominações legais, com validade durante toda a execução do contrato e até 03 (três) meses após o término da vigência contratual, na forma prescrita no art. 158, inciso II, alíneas “a” a “d”, do Regulamento de Licitações e Contratos – RLC da CONTRATANTE.

§3º A CONTRATADA ficará obrigada a repor o valor da garantia quando esta for utilizada, bem como a atualizar o seu valor nas mesmas condições do contrato.

§4º No caso de seguro-garantia ou fiança bancária, não será admitida a existência de cláusulas que restrinjam ou atenuem a responsabilidade do segurador ou fiador.

§5º A CONTRATADA deverá atualizar a garantia sempre que houver alteração contratual, no mesmo prazo deferido para a comprovação da garantia originária, visando assegurar a cobertura das modificações procedidas.

§6º Será recusada a garantia que não atender às especificações, sendo facultada à CONTRATADA apresentar caução em dinheiro, no prazo de 05 (cinco) dias, contados da notificação da recusa pela CONTRATANTE.

§7º A inobservância dos prazos fixados nesta Cláusula para apresentação da garantia acarretará a aplicação de multa de 10% (dez por cento) sobre o valor deste contrato.

§8º O atraso superior a 25 (vinte e cinco) dias para apresentação da garantia por parte da CONTRATADA autoriza a CONTRATANTE adotar as seguintes providências:

- a) promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas obrigações;
- b) reter o valor da garantia dos pagamentos eventualmente devidos a CONTRATADA até que a garantia seja apresentada.

§9º A garantia será extinta nas hipóteses indicadas no art. 159, incisos I e II, §§ 1º e 2º do Regulamento de Licitações e Contratos da PRODEB.

CLÁUSULA OITAVA - MANUTENÇÃO DAS CONDIÇÕES DA PROPOSTA – REAJUSTAMENTO E REVISÃO

Os preços são fixos e irreajustáveis durante o transcurso do prazo de 12 meses da data de apresentação da proposta, após o que a concessão de reajustamento, será feita mediante a aplicação do **INPC/IBGE**, conforme orientações traçadas no art. 176 do Regulamento de Licitações e Contratos – RLC da PRODEB.

§1º A revisão de preços, nos termos do art. 178 do Regulamento de Licitações e Contratos – RLC da PRODEB, dependerá de requerimento da CONTRATADA quando visar recompor o preço que se tornou *insuficiente*, instruído com a documentação que comprove o desequilíbrio econômico-financeiro do contrato, devendo ser instaurada pela própria CONTRATANTE quando colimar recompor o preço que se tornou *excessivo*.

§2º O requerimento de revisão de preços deverá ser formulado pela CONTRATADA no prazo máximo de um ano a partir do fato que a ensejou, sob pena de decadência, em consonância com o art. 211 da Lei 10.406/02.

§3º A variação do valor contratual para fazer face ao reajuste de preços previsto no próprio contrato, quando for o caso, as atualizações, compensações ou apenações financeiras decorrentes das condições de pagamento nele previstas, bem como o empenho de dotações orçamentárias suplementares até o limite do seu valor corrigido, não caracterizam alteração do mesmo, podendo ser registrados por simples apostila, dispensando a celebração de aditamento.

§4º Os preços contratuais não serão reajustados em caso de atrasos verificados e não justificados por parte da CONTRATADA que influenciem no prazo contratual ou cujas justificativas não forem aceitas pela CONTRATANTE.

§5º Os reajustes, repactuações e revisões que não forem solicitadas durante a vigência do ajuste serão objeto de preclusão com a assinatura da prorrogação ou renovação ou com o encerramento deste contrato.

CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATADA

A **CONTRATADA**, além das determinações contidas nos **ANEXOS I e II** do presente instrumento, em especial as constantes nos **itens 22, 23, 25.1 (Lote1), 28 (Lote1) e 29 do Termo de Referência**, que aqui se consideram literalmente transcritas, bem como daquelas decorrentes de lei, obriga-se a:

- a) designar de sua estrutura administrativa um preposto permanentemente responsável pela perfeita execução dos serviços, inclusive para atendimento de emergência, bem como para zelar pela prestação contínua e ininterrupta dos serviços, bem como, dentre os que permaneçam no local do trabalho, um que será o responsável pelo bom andamento dos serviços e que possa tomar as providências pertinentes para que sejam corrigidas todas as falhas detectadas;
- b) executar os serviços objeto deste contrato de acordo com as especificações ou recomendações efetuadas pela CONTRATANTE;
- c) manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e recursos humanos para execução completa e eficiente dos serviços objeto deste contrato;
- d) zelar pela boa e completa execução dos serviços contratados e facilitar, por todos os meios ao seu alcance, a ampla ação fiscalizadora dos prepostos designados pela CONTRATANTE, atendendo prontamente às observações e exigências que lhe forem solicitadas;
- e) comunicar a CONTRATANTE qualquer anormalidade que interfira no bom andamento dos serviços;
- f) atender com presteza as reclamações sobre a qualidade dos serviços executados, providenciando sua imediata correção, sem ônus para a CONTRATANTE;
- g) respeitar e fazer com que seus empregados respeitem as normas de segurança do trabalho, disciplina e demais regulamentos vigentes na CONTRATANTE, bem como atentar para as regras de cortesia no local onde serão executados os serviços;
- h) reparar, repor ou restituir, nas mesmas condições e especificações, dentro do prazo que for determinado, os equipamentos e utensílios eventualmente recebidos para uso nos serviços objeto deste contrato, deixando as instalações na mais perfeita condição de funcionamento;
- i) arcar com todo e qualquer dano ou prejuízo de qualquer natureza causado a CONTRATANTE e terceiros, por sua culpa, ou em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir o equivalente a todos os danos decorrentes de paralisação ou interrupção dos serviços contratados, exceto quando isto ocorrer por exigência da CONTRATANTE ou ainda por caso fortuito ou força maior, circunstâncias que deverão ser comunicadas no prazo de 48 (quarenta e oito) horas após a sua ocorrência;
- j) manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- k) providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes, necessários à execução dos serviços;
- l) efetuar pontualmente o pagamento de todas as taxas e impostos que incidam ou venham a incidir sobre as suas atividades e/ou sobre a execução do objeto do presente contrato, bem como observar e respeitar as Legislações Federal, Estadual e Municipal, relativas aos serviços prestados;
- m) respeitar todas as obrigações consignadas no Termo de Referência que constitui o **ANEXO I** deste Contrato, independentemente de transcrição;
- n) cumprir, durante todo o período de execução do Contrato, a reserva de cargos prevista em lei, observado o disposto no art. 157, XIX do RLC/PRODEB;
- o) atender às seguintes obrigações concernentes à aprendizagem: [art. 157, XIX do RLC/PRODEB c/c Lei nº 13.459/15 e Decreto nº 16.761/15]:
 - i. observar a determinação do art. 429 do Decreto-Lei nº 5.452, de 1943 (Consolidação das Leis do Trabalho - CLT) e respectiva regulamentação;
 - ii. recrutar, preferencialmente, para a contratação de aprendizes determinada pelo art. 429 da CLT, os estudantes indicados no §2º do art. 38 da Lei estadual nº 14.395, de 2021, no percentual mínimo de 10% (dez por cento) do quadro de aprendizes da CONTRATADA;
 - iii. apresentar ao fiscal ou responsável pela gestão e acompanhamento do contrato, no prazo de até 05 (cinco) dias úteis contado do início efetivo da execução do serviço, a lista completa dos aprendizes, indicando aqueles selecionados no banco de dados de que trata a Lei estadual nº 14.395, de 2021, devendo justificar, perante o CONTRATANTE, a eventual impossibilidade

de seu cumprimento.

- p) comprovar a reserva de cargos a que se refere o subitem acima, no prazo fixado pelo CONTRATANTE, com a indicação dos empregados que preencheram as referidas vagas;
- q) cumprir, durante todo o período de execução do Contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, devendo, sempre que solicitado pelo Contratante, indicar os empregados que preencherem as vagas correspondentes (arts. 92, inc. XVIII, e 116 da Lei Federal nº 14.133/2021).

CLÁUSULA DÉCIMA - OBRIGAÇÕES DA CONTRATANTE

A **CONTRATANTE**, além das obrigações contidas neste contrato por determinação legal e nos **itens 24, 25.3 (Lote 1) do Termo de Referência**, obriga-se a:

- a) fornecer a CONTRATADA os elementos indispensáveis ao cumprimento do contrato;
- b) realizar o pagamento pela execução do contrato;
- c) proceder à publicação resumida do instrumento de contrato, de seus aditamentos e apostilamentos na imprensa oficial e no sítio eletrônico da PRODEB no prazo legal;
- d) disponibilizar, em sua sede, os equipamentos e materiais necessários para uso dos colaboradores da CONTRATADA;
- e) liberar senhas de acesso para que os colaboradores da CONTRATADA utilizem a rede interna e externa, quando for o caso;
- f) comunicar qualquer irregularidade identificada durante a execução das atividades, possibilitando a pronta regularização da situação por parte da CONTRATADA;
- g) cumprir pontualmente com o compromisso financeiro assumido neste contrato nos prazos e condições ajustados na Cláusula Sexta deste instrumento.

CLÁUSULA DÉCIMA PRIMEIRA - REGIME DE EXECUÇÃO

O regime de execução do presente contrato é de empreitada por preço **unitário**.

CLÁUSULA DÉCIMA SEGUNDA – DA PROTEÇÃO DE DADOS PESSOAIS

A CONTRATADA obriga-se ao dever de proteção, confidencialidade e sigilo de toda informação, dados pessoais e/ou base de dados a que tenha acesso, nos termos da Lei nº 13.709/2018, suas alterações e regulamentações posteriores, durante o cumprimento do objeto descrito no presente instrumento contratual de acordo com as condições a seguir e conforme disposto no item **23 do Termo de Referência**.

§1º A CONTRATADA obriga-se a implementar medidas técnicas e administrativas suficientes visando a segurança, a proteção, a confidencialidade e o sigilo de toda informação, dados pessoais e/ou base de dados a que tenha acesso a fim de evitar acessos não autorizados, acidentes, vazamentos acidentais ou ilícitos que causem destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento não previstos.

§2º A CONTRATADA deve assegurar-se de que todos os seus colaboradores, consultores e/ou prestadores de serviços que, no exercício das suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, respeitem o dever de proteção, confidencialidade e sigilo.

§3º A CONTRATADA não poderá utilizar-se de informação, dados pessoais e/ou base de dados a que tenha acesso, para fins distintos ao cumprimento do objeto deste instrumento contratual.

§4º A CONTRATADA não poderá disponibilizar e/ou transmitir a terceiros, sem prévia autorização escrita, informação, dados pessoais e/ou base de dados a que tenha acesso em razão do cumprimento do objeto deste instrumento contratual.

a) a CONTRATADA obriga-se a fornecer apenas a informação, dados pessoais e/ou base de dados estritamente necessários quando da transmissão autorizada a terceiros durante o cumprimento do objeto descrito neste instrumento contratual.

§5º A CONTRATADA fica obrigada a excluir ou devolver, a critério da contratante, todos os documentos, registros e cópias que contenham informação, dados pessoais e/ou base de dados a que tenha tido acesso durante a execução do objeto deste instrumento contratual no prazo de 30 (trinta) dias corridos, contados

da data da ocorrência de qualquer uma das hipóteses de extinção do contrato, restando autorizada a conservação apenas nas hipóteses legalmente previstas.

a) à CONTRATADA não será permitido deter cópias ou *backups*, informação, dados pessoais e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual.

b) a CONTRATADA deverá eliminar os dados pessoais a que tiver conhecimento ou posse em razão do cumprimento do objeto deste instrumento contratual tão logo não haja mais necessidade de realizar seu tratamento.

§6º A CONTRATADA deverá notificar imediatamente a CONTRATANTE em caso de vazamento ou perda parcial ou total de informação, dados pessoais e/ou base de dados.

a) a notificação não eximirá A CONTRATADA das obrigações e/ou sanções que possam incidir em razão da perda de informação, dados pessoais e/ou base de dados.

§7º A CONTRATADA que descumprir os termos da Lei nº 13.709/2018 suas alterações e regulamentações posteriores, durante ou após a execução do objeto descrito no presente instrumento contratual fica obrigada a assumir total responsabilidade e ao ressarcimento por todo e qualquer dano e/ou prejuízo sofrido, incluindo sanções aplicadas pela autoridade competente.

§8º A CONTRATADA fica obrigada a manter preposto para comunicação com CONTRATANTE para os assuntos pertinentes à Lei nº 13.709/2018 suas alterações e regulamentações posteriores.

§9º O dever de sigilo e confidencialidade, e as demais obrigações descritas na presente cláusula, permanecerão em vigor após a extinção das relações entre A CONTRATADA e a CONTRATANTE, bem como, entre A CONTRATADA e os seus colaboradores, subcontratados, consultores e/ou prestadores de serviços sob pena das sanções previstas na Lei nº 13.709/2018, suas alterações e regulamentações posteriores, salvo decisão judicial contrária.

§10º O não cumprimento de quaisquer das obrigações descritas nesta cláusula sujeitará A CONTRATADA a processo administrativo para apuração de responsabilidade e, consequente, sanção, sem prejuízo de outras penalidades.

CLÁUSULA DÉCIMA TERCEIRA – GESTÃO, FISCALIZAÇÃO DO CONTRATO E RECEBIMENTO DO OBJETO

Competirá a CONTRATANTE proceder ao acompanhamento da execução do contrato, na forma dos artigos 185 a 201 do Regulamento de Licitações e Contratos – RLC da PRODEB e item 26 do Termo de Referência, ficando esclarecido que a ação ou omissão, total ou parcial, da fiscalização da CONTRATANTE não eximirá à CONTRATADA de total responsabilidade na execução do contrato.

§1º O adimplemento da obrigação contratual por parte da CONTRATADA ocorre com a efetiva prestação do serviço, a realização da obra, a entrega do bem, assim como qualquer outro evento contratual cuja ocorrência esteja vinculada à emissão de documento de cobrança.

§2º Cumprida a obrigação pela CONTRATADA, caberá a CONTRATANTE, proceder ao recebimento do objeto, a fim de aferir os serviços ou fornecimentos efetuados, para efeito de emissão da habilitação de pagamento.

§3º O recebimento do objeto se dará segundo o disposto nos artigos 197 a 201 do Regulamento de Licitações e Contratos – RLC da PRODEB, observando-se os seguintes prazos, se **outros não houverem sido fixados nos ANEXOS do presente contrato.**

- a) se a verificação da conformidade do objeto com a especificação, bem assim do cumprimento das obrigações acessórias puder ser realizada de imediato, será procedido de logo o recebimento definitivo;
- b) quando, em razão da natureza, do volume, da extensão, da quantidade ou da complexidade do objeto, não for possível proceder-se a verificação imediata de conformidade, será feito o recebimento provisório, devendo ser procedido ao recebimento definitivo no prazo de 15 (quinze) dias.

§4º O recebimento definitivo do objeto contratado, cujo valor seja superior ao dobro do valor estabelecido no inciso II do artigo 34 do Regulamento de Licitações e Contratos – RLC da PRODEB, deverá ser confiado a uma comissão de, no mínimo, 03 (três) membros.

§5º A CONTRATANTE rejeitará, no todo ou em parte, qualquer proposição de serviços/obras/bens em desconformidade com as especificações constantes do Termo de Referência ou Projeto Básico e das disposições previstas neste Contrato.

§6º Esgotado o prazo total para conclusão do recebimento definitivo sem qualquer manifestação da CONTRATANTE, considerar-se-á definitivamente aceito o objeto contratual, para todos os efeitos.

§7º Com a conclusão da etapa do recebimento definitivo, a CONTRATADA estará habilitada a apresentar as nota(s) fiscal(is)/fatura(s) para pagamento, acompanhada dos documentos comprobatórios da regularidade fiscal e trabalhista.

§8º Fica indicado como Gestor do presente contrato XXXXXXXXX, Titular da XXXXXXXX, matrícula nº XXXXXXXX e como Fiscal XXXXXX, XXXXXXXXXXXX, matrícula nº XXXXXXXXXXXX.

§9º A execução do contrato deverá ser acompanhada e fiscalizada pelos representantes da CONTRATANTE especialmente designados no parágrafo antecedente.

§10º Os representantes da CONTRATANTE anotarão em registro próprio todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados.

§11º As decisões e providências que ultrapassarem a competência dos representantes deverão ser solicitadas aos seus superiores em tempo hábil para adoção de medidas pertinentes.

CLÁUSULA DÉCIMA QUARTA – PENA DE MULTA

A inexecução contratual, inclusive por atraso injustificado na execução do contrato, ensejará a aplicação da pena de multa prevista no artigo 212, II, do Regulamento de Licitações e Contratos – RLC da PRODEB, observados os parâmetros estabelecidos nesta cláusula, sem prejuízo da resolução do contrato (artigo 205 do Regulamento de Licitações e Contratos – RLC da PRODEB), a qualquer tempo, e a aplicação das demais sanções previstas no citado RLC.

§1º Multa compensatória:

- a) No caso de descumprimento total da obrigação principal, será aplicada multa compensatória no percentual de 15% (quinze por cento) incidente sobre o valor global do contrato.
- b) Caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicada multa compensatória no percentual de 15% (quinze por cento) incidente sobre o saldo do contrato, isto é, sobre a diferença entre o valor global do contrato e o valor da parte do serviço já realizado.
- c) No caso de descumprimento da obrigação acessória, será aplicada multa compensatória no percentual de 15% (quinze por cento) incidente sobre o valor da obrigação descumprida ou da estimativa arbitrada do seu custo.
- d) No caso de recusa injustificada do adjudicatário em assinar o termo de contrato, em aceitar ou retirar o instrumento equivalente, ou, quando for o caso, em assinar a ata de registro de preços, ou praticar condutas a elas equiparadas, será aplicada multa compensatória no percentual de 15% (quinze por cento) incidente sobre o valor correspondente ao objeto adjudicado ou, quando for o caso, da estimativa da contratação.
- e) Considera-se acessória, para os fins deste Contrato, a obrigação contratual de natureza instrumental, secundária ou meramente formal.
- f) O inadimplemento de obrigação acessória que retarde, comprometa ou impeça a execução da obrigação principal será considerado descumprimento da obrigação principal, sujeitando-se às cominações legais respectivas.

§2º Multa moratória:

- a) O atraso injustificado na execução do Contrato ensejará a aplicação de multa moratória no percentual de 0,1% (um décimo por cento) ao dia, incidente sobre o valor da obrigação descumprida ou da estimativa arbitrada do seu custo, observado o percentual máximo total de 30% (trinta por cento).
- b) O atraso injustificado do prazo fixado para apresentação, suplementação ou reposição de garantia contratual ensejará a aplicação de multa moratória no percentual de 0,1% (um décimo por cento) ao dia, incidente sobre o valor global do contrato.
- c) A aplicação de multa de mora não impedirá que a PRODEB a converta em compensatória e promova a extinção unilateral do Contrato com a aplicação cumulada de outras sanções previstas no RLC/PRODEB.
- d) Na hipótese do subitem anterior, se o cálculo da multa moratória atingir o patamar correspondente ao valor máximo da multa compensatória, o recebimento do objeto deverá ser recusado, salvo justificativa escrita devidamente fundamentada, sem prejuízo da aplicação das demais sanções previstas no RLC/PRODEB.

§3º As multas previstas nestes parágrafos não têm caráter compensatório e o seu pagamento não eximirá a CONTRATADA da responsabilidade por perdas e danos decorrentes das infrações cometidas.

§4º Caso a multa aplicada não cubra os prejuízos causados pela CONTRATADA, a CONTRATANTE pode exigir indenização suplementar, valendo a multa como mínimo de indenização, na forma do preceituado no parágrafo único do artigo 416 do Código Civil.

§5º A multa, aplicada após regular processo administrativo, será descontada da garantia da CONTRATADA faltosa, sendo certo que, se o seu valor exceder ao da garantia prestada – quando exigida, além da perda desta, a CONTRATADA responderá pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela CONTRATANTE ou, ainda, se for o caso, cobrada judicialmente. Acaso não tenha sido exigida garantia, à CONTRATANTE se reserva o direito de descontar diretamente do pagamento devido à CONTRATADA o valor de qualquer multa porventura imposta, conforme artigo 203, § 13º, do Regulamento de Licitações e Contratos – RLC da PRODEB.

§6º A personalidade jurídica da CONTRATADA poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos em lei e neste Contrato ou para provocar confusão patrimonial.

- a) com a desconsideração da personalidade jurídica, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a CONTRATADA;
- b) em todos os casos de desconsideração da personalidade jurídica deverão ser observados o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art.225 do RLC/PRODEB).

§7º O CONTRATANTE deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

- a) as sanções de impedimento de licitar e contratar são passíveis de reabilitação;
- b) a apuração das infrações administrativas será realizada em processo administrativo sancionatório, com a observância das garantias da ampla defesa e do contraditório, na forma do regulamento.

CLÁUSULA DÉCIMA QUINTA – OUTRAS PENALIDADES

Serão punidos com a pena de suspensão temporária do direito de licitar e impedimento de contratar com a CONTRATANTE os que incorrerem nos ilícitos previstos nos incisos II a XVI do art. 211 do RLC/PRODEB.

§1º A sanção de advertência é cabível sempre que o ato praticado, ainda que configure a violação de preceito contratual ou legal, não seja suficiente para acarretar danos à CONTRATANTE, seus processos, suas instalações, pessoas, imagem, meio ambiente ou a terceiros, e não se justificar a imposição de penalidade mais grave.

§2º Para a aplicação das penalidades previstas serão levados em conta a natureza e a gravidade da falta, os prejuízos dela advindos para a CONTRATANTE, na forma do que prescreve o §2º do artigo 212 do RLC-PRODEB.

CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

Poderá haver alteração contratual, mediante acordo formal entre as partes, nos seguintes casos:

- a) quando houver modificação do projeto ou das especificações, para melhor adequação técnica aos seus objetivos;
- b) quando necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites permitidos pela Lei nº 13.303/2016 e Regulamento de Licitações e Contratos – RLC da PRODEB;
- c) quando conveniente a substituição da garantia de execução;
- d) quando necessária a modificação do regime de execução da obra ou serviço, bem como do modo de fornecimento, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;
- e) para restabelecer a relação que as partes pactuaram inicialmente entre os encargos da CONTRATADA e a retribuição da CONTRATANTE para a justa remuneração da obra, serviço ou fornecimento, objetivando a manutenção do equilíbrio econômico-financeiro inicial do contrato, na hipótese de sobrevirem fatos imprevisíveis, ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

§1º A CONTRATADA poderá aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem no objeto contratado, até 25% (vinte e cinco por cento) do valor inicial atualizado deste ajuste, e, no caso particular de reforma de edifício ou de equipamento, até o limite de 50% (cinquenta por cento) para os seus acréscimos.

§2º Nenhum acréscimo ou supressão poderá exceder os limites estabelecidos no §1º desta cláusula, salvo as supressões resultantes de acordo celebrado entre CONTRATANTE e CONTRATADA.

§3º A criação, a alteração ou a extinção de quaisquer tributos ou encargos legais, bem como a superveniência de disposições legais, quando ocorridas após a data da apresentação da proposta, com comprovada repercussão nos preços contratados, implicarão a revisão destes para mais ou para menos, conforme o caso.

§4º Em havendo alteração do contrato que aumente os encargos da CONTRATADA, a CONTRATANTE deverá restabelecer, por aditamento, o equilíbrio econômico-financeiro inicial, desde que devidamente justificado.

§5º A variação do valor contratual para fazer face ao reajuste de preços previsto neste contrato e as atualizações, compensações ou penalizações financeiras decorrentes das condições de pagamento nele previstas, bem como o empenho de dotações orçamentárias suplementares até o limite do seu valor corrigido, não caracterizam alteração do contrato e podem ser registrados por apostila, dispensada a celebração de aditamento.

§6º É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados na matriz de risco como de responsabilidade da CONTRATADA.

CLÁUSULA DÉCIMA SÉTIMA – RESCISÃO

Constituem motivos que autorizam a CONTRATANTE exercer o direito de resolução deste contrato, independentemente de provimento judicial ou extrajudicial nesse sentido:

- a) descumprimento total ou parcial de obrigações pela CONTRATADA;
- b) alteração social ou modificação da finalidade ou da estrutura da CONTRATADA, se, a juízo da CONTRATANTE, prejudicar a execução do ajuste;
- c) retardamento injustificado do início da execução deste contrato pela CONTRATADA;
- d) mora na execução deste contrato, levando a CONTRATANTE a comprovar a impossibilidade da conclusão do objeto deste contrato, nos prazos pactuados;

- e) paralisação, total ou parcial, da execução do objeto contratado sem justa causa previamente comunicada à CONTRATANTE;
- f) subcontratação parcial do objeto, a associação da CONTRATADA com outrem, a cessão ou transferência, total ou parcial deste contrato, bem como a fusão, cisão ou incorporação da CONTRATADA, não admitidas por este contrato;
- g) desatendimento reiterado às determinações regulares do Gestor e Fiscais deste contrato;
- h) cometimento reiterado de faltas na execução contratual, anotadas pelo Gestor e Fiscais deste contrato;
- i) falta de integralização da garantia contratual nos prazos estipulados;
- j) descumprimento da vedação de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e de qualquer trabalho a menores de 16 (dezesesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos;
- k) superveniência da declaração de inidoneidade para licitar e contratar com a Administração;
- l) perecimento do objeto contratual, tornando impossível o prosseguimento da execução da avença;
- m) declaração de falência ou instauração da insolvência civil;
- n) dissolução da sociedade ou falecimento da CONTRATADA;
- o) ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do contrato;
- p) impossibilidade de alteração do valor do contrato por recusa da CONTRATADA quando possível a redução do preço ajustado para compatibilizá-lo ao valor de mercado ou quando houver diminuição, devidamente comprovada, dos preços dos insumos básicos utilizados no contrato;
- q) quando a CONTRATADA for envolvida em casos de corrupção ou sobre os quais haja forte suspeita de envolvimento, condicionada à prévia manifestação da área de compliance da CONTRATANTE;
- r) quando a CONTRATADA não manter as condições de habilitação e qualificação durante a execução deste contrato.

§1º As hipóteses de resolução contratual previstas nesta cláusula devem ser formalmente motivadas em processo administrativo pela CONTRATANTE na forma das orientações traçadas na Lei nº 12.209/2011, sendo assegurada à CONTRATADA o contraditório e a ampla defesa prévios.

§2º Quando a resolução deste contrato ocorrer por ato unilateral da CONTRATANTE, acarretará as consequências previstas no artigo 205, §2º, do Regulamento de Licitações e Contratos – RLC da PRODEB, sem prejuízo da aplicação das sanções previstas neste contrato e no citado RLC.

§3º Quando a resolução do contrato ocorrer sem que haja culpa da CONTRATADA, esta será ressarcida dos prejuízos que houver sofrido, desde que regularmente comprovados, e ainda terá direito a:

- a) devolução da garantia, se houver;
- b) pagamentos devidos pela execução deste contrato até a data da rescisão;
- c) pagamento do custo da desmobilização, se houver, hipótese em que deve ser requerido e devidamente comprovado pela CONTRATADA.

§4º A extinção deste contrato poderá ocorrer nas formas previstas no artigo 204 do Regulamento de Licitações e Contratos – RLC da PRODEB.

CLÁUSULA DÉCIMA OITAVA – MATRIZ DE RISCO

Na hipótese de ocorrência de um dos eventos listados no ANEXO III – MATRIZ DE RISCO deste contrato, a CONTRATADA deverá, no prazo de 24 (vinte e quatro) horas, informar a CONTRATANTE sobre o ocorrido, contendo, no mínimo, os seguintes dados:

- a) detalhamento do evento ocorrido, incluindo a sua natureza, a data da ocorrência e sua duração estimada;
- b) as medidas que estavam em vigor para mitigar o risco de materialização do evento, quando houver;
- c) as medidas que irá adotar para fazer cessar os efeitos do evento e o prazo estimado para que esses efeitos cessem;
- d) as obrigações contratuais que não foram cumpridas ou que não irão ser cumpridas em razão do evento; e

e) demais esclarecimentos e informações relevantes.

§1º Após a notificação da CONTRATADA da ocorrência de que trata esta cláusula, a CONTRATANTE decidirá quanto ao ocorrido, podendo, para tanto, solicitar esclarecimentos adicionais a CONTRATADA. Em sua decisão a CONTRATANTE poderá isentar temporariamente a CONTRATADA do cumprimento das obrigações contratuais afetadas pelo evento.

§2º A concessão de isenção aludida no §1º desta cláusula não exclui a possibilidade de aplicação das sanções previstas neste contrato pela CONTRATANTE.

§3º O reconhecimento pela CONTRATANTE dos eventos descritos no ANEXO IV deste contrato que afetem o cumprimento das obrigações contratuais, com responsabilidade indicada exclusivamente a CONTRATADA, não dará ensejo a recomposição do equilíbrio econômico-financeiro deste contrato, devendo o risco ser suportado exclusivamente pela CONTRATADA.

§4º As obrigações contratuais afetadas por caso fortuito, fato do príncipe ou força maior deverão ser comunicadas pelas partes em até 24 (vinte e quatro) horas, contados da data da ocorrência do evento.

§5º Nas hipóteses indicadas no parágrafo precedente as partes deverão acordar a forma e o prazo para resolução do ocorrido.

§6º As partes não serão consideradas inadimplentes em razão do descumprimento contratual decorrente de caso fortuito, fato do príncipe ou força maior.

§7º Avaliada a gravidade do evento nas hipóteses indicadas no §4º desta cláusula, as partes, mediante acordo, decidirão quanto à recomposição do equilíbrio econômico-financeiro deste contrato, salvo se as consequências do evento sejam cobertas por seguro, se houver.

§8º Este contrato poderá ser rescindido, quando demonstrado que todas as medidas para sanar os efeitos do evento foram adotadas e mesmo assim a manutenção da avença se torna impossível ou inviável nas condições existentes ou é excessivamente onerosa.

§9º As partes se comprometem a empregar e exaurir todas as medidas e ações necessárias para minimizar os efeitos advindos dos eventos de caso fortuito, fato do príncipe ou força maior.

§10º Os fatos imprevisíveis, ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução deste contrato, não previstos no ANEXO III – MATRIZ DE RISCOS, serão decididos mediante acordo entre as partes, no que diz respeito à recomposição do equilíbrio econômico-financeiro do ajuste.

CLÁUSULA DÉCIMA NONA - VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO

Integram o presente contrato, como se nele estivessem transcritas, as cláusulas e condições estabelecidas no processo licitatório, referido no preâmbulo deste instrumento, inclusive anexos e adendos, e na proposta da licitante vencedora.

CLÁUSULA VIGÉSIMA - COMUNICAÇÃO ELETRÔNICA

Fica pactuado que os atos de comunicação processual com a CONTRATADA poderão ser realizados por meio eletrônico, na forma do disposto na Lei nº 12.209, de 20 de abril de 2011, e do Decreto nº 15.805, de 30 de dezembro de 2014.

Parágrafo único. A CONTRATADA deverá manter atualizado o endereço eletrônico cadastrado no Sistema Eletrônico de Informações - SEI, para efeito do recebimento de notificação e intimação de atos processuais.

CLÁUSULA VIGÉSIMA PRIMEIRA – DISPOSIÇÕES FINAIS

Qualquer tolerância de uma das partes na exigência do cumprimento do presente contrato não constituirá novação, renúncia tácita ou extinção da respectiva obrigação, podendo a mesma ser exigida a qualquer tempo.

CLÁUSULA VIGÉSIMA SEGUNDA – DOCUMENTOS COMPLEMENTARES

Os seguintes documentos, na ordem adiante relacionados, constituem anexos deste contrato. Os termos deste contrato, em caso de dúvidas, prevalecerão sobre os anexos:

ANEXO I – TERMO DE REFERÊNCIA

ANEXO II – PROPOSTA DA CONTRATADA

ANEXO III – MATRIZ DE RISCOS

ANEXO IV – GARANTIA

CLÁUSULA VIGÉSIMA TERCEIRA – FORO

As partes elegem o Foro da Cidade do Salvador, Estado da Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para solucionar quaisquer dúvidas oriundas deste instrumento que não puderem ser dirimidas por quaisquer dos meios alternativos resolução de controvérsias.

E, por estarem assim justos e contratados, firmam o presente contrato.

Salvador, ____ de _____ de 2026.

Pela **CONTRATANTE/PRODEB:**

José Muniz Rebouças
Diretor Executivo

Carlos Augusto Borges Silva
Diretor de Infraestrutura Tecnológica e Conectividade

Pela **CONTRATADA:**

Nome Representante: XXXXX
Fornecedor: XXXXX

MINUTA DEMAIS ÓRGÃOS E ENTIDADES

**CONTRATO Nº ____/____ QUE ENTRE SI CELEBRAM O
[ESTADO DA BAHIA] [AUTARQUIA _____] [FUNDÇÃO] E A [PESSOA JURÍDICA/PESSOA FÍSICA]
_____, PARA OS FINS QUE NELE SE DECLARAM.**

O **ESTADO DA BAHIA**, neste ato representado pelo(a) Dr(a). _____, titular da Secretaria _____, CNPJ nº _____, situada na _____, autorizado pelo Decreto de delegação de competência publicado no D.O.E. de ____/____/____, doravante denominado Contratante, [utilizar a menção ao Estado somente se for órgão da Administração Direta]

OU

A [autarquia ou fundação], situada na _____, inscrita no CNPJ sob o nº _____, neste ato representada pelo(a) _____ [cargo e nome], portador da cédula de identidade nº _____, emitida por _____, inscrito no CPF/MF sob o nº _____, doravante denominado Contratante

e a _____ [pessoa jurídica], inscrita no CNPJ/MF sob o nº _____, sediada na _____, doravante representada pelo Sr(a). _____, portador da cédula de identidade nº _____, emitida por _____, inscrito(a) no CPF/MF sob o nº _____, conforme atos constitutivos da empresa ou procuração apresentada nos autos, doravante denominada Contratada, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico nº 005/2026 processado e conduzido pela Companhia de Processamento de Dados do Estado da Bahia – PRODEB, conforme Termo de Cooperação Técnica nº 002/2026 celebrado entre o Estado da Bahia, por intermédio da Secretaria da Administração e a PRODEB, processo administrativo nº 065.10933.2026.0003946-61, que se regerá pela Lei nº 14.634, de 28 de novembro de 2023, pela Lei Federal nº 14.133, de 1º de abril de 2021, e mediante as cláusulas e condições a seguir ajustadas.

CLÁUSULA PRIMEIRA – OBJETO

- 1.1 O objeto do presente instrumento é a contratação dos serviços/fornecimento especificados no(s) **Lote 1/Lote 2**, nas condições estabelecidas no Termo de Referência (TR).
- 1.2 Vinculam-se a esta contratação, independentemente de transcrição neste instrumento:
- a) Termo de Referência;
 - b) Proposta da Contratada;
 - c) Edital da Licitação;
 - d) Eventuais anexos dos documentos supracitados.

1.3 O modelo de execução do objeto observará o disposto no Termo de Referência.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1 **LOTE 1:** O prazo de vigência do Contrato é de 05 (cinco) anos, considerando a natureza dos serviços contínuos, e a maior vantagem econômica para a Administração em razão da contratação plurianual prevista; podendo ser prorrogado até o limite de 10 (dez) anos, desde que atestada a vantajosidade econômica e a regularidade fiscal/trabalhista da contratada, nos termos do art. 107 da Lei nº 14.133/2021, conforme item 21.1.1 do TR.

LOTE 2: O prazo de vigência do Contrato é de 12 (doze) meses, podendo ser prorrogados, por sucessivo (s) período (s), até atingir o limite de 05 (cinco) anos, nos termos do art. 106 da Lei Federal nº 14.133/2021, conforme item 21.2 do TR.

2.2 A prorrogação de que trata esta Cláusula está condicionada à justificativa e autorização da autoridade competente para celebrar o ajuste, devendo as condições e preços permanecerem vantajosos para o Contratante, permitida a negociação com a Contratada, observando-se, ainda, o cumprimento dos seguintes requisitos:

- a) comprovação de que a forma de execução do objeto tem natureza continuada;
- b) apresentação de relatório que discorra sobre a execução do Contrato e sua regularidade;
- c) apresentação de justificativa e motivo, por escrito, de que a Administração mantém interesse na continuidade da execução contratual;
- d) manifestação expressa da Contratada informando o interesse na prorrogação;
- e) comprovação de que a Contratada mantém as condições iniciais de habilitação.

2.3 A Contratada não tem direito subjetivo à prorrogação contratual.

2.4 A prorrogação do Contrato deverá ser promovida mediante celebração de termo aditivo.

2.5 Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

2.6 O Contrato não poderá ser prorrogado, quando for aplicada à Contratada (art. 44, §3º, inc. III, do Decreto nº 23.113, de 9 de outubro de 2024):

- a) a sanção de impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do Estado da Bahia;
- b) a sanção de declaração de inidoneidade para licitar e contratar, nos termos do art. 156, §5º, da Lei Federal nº 14.133/2021.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

3.1 As regras de execução e de gestão do contrato constam no Termo de Referência, anexo a este Contrato (art. 92 da Lei Federal nº 14.133/2021).

3.2 Fica indicado como gestor deste Contrato o servidor _____, matrícula:

3.3 Fica(m) indicado(s) como fiscal(is) deste Contrato o(s) servidor(es): _____
matrícula(s): _____

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

Lote 1:

4.1 É admitida a subcontratação parcial do objeto, nas condições indicadas **nos itens 16.1 a 16.9 do TR.**

4.1.1 Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante o Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação, não se responsabilizando o Contratante por nenhum compromisso assumido pela Contratada com terceiros.

4.1.2 A subcontratação depende de autorização prévia do Contratante, a quem incumbe avaliar se a subcontratada cumpre os requisitos de qualificação técnica necessários para a execução do objeto (art. 122, §1º, da Lei Federal nº 14.133/2021).

4.1.2.1 A Contratada apresentará à Administração documentação que comprove a capacidade técnica da subcontratada, que será avaliada e juntada aos autos do processo correspondente (art. 122, §1º, da Lei Federal nº 14.133/2021).

4.1.3 É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou da entidade contratante ou com agente público que desempenhe função na contratação ou atue na fiscalização ou na gestão do Contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau (art. 122, §3º, da Lei Federal nº 14.133/2021).

4.1.4 Caso tenha sido formulada no TR a exigência de subcontratação de microempresas ou empresas de pequeno porte (art. 48, inc. II, da Lei Complementar nº 123/2006), além do regramento acima, deverão ser observadas as seguintes disposições específicas:

- a) a Contratada deverá apresentar, ao longo da vigência contratual, sempre que solicitada, a documentação de regularidade fiscal das microempresas e empresas de pequeno porte subcontratadas, sob pena de extinção do Contrato, assegurando-lhe, para fins de regularização, o prazo de 5 (cinco) dias úteis, prorrogável por até igual período;
- b) a Contratada deverá substituir a subcontratada, no prazo máximo de 30 (trinta) dias, na hipótese de extinção da subcontratação, mantendo o percentual originalmente subcontratado até a sua execução total, notificando o Contratante, sob pena de extinção contratual, sem prejuízo das sanções cabíveis, ou a demonstrar a inviabilidade da substituição, hipótese em que ficará responsável pela execução da parcela originalmente subcontratada;
- c) a Contratada será responsável pela padronização, pela compatibilidade, pelo gerenciamento centralizado e pela qualidade da subcontratação; e

d) os empenhos e pagamentos referentes às parcelas subcontratadas serão destinados diretamente às microempresas e empresas de pequeno porte subcontratadas (art. 48, §2º, da Lei Complementar nº 123/2006).

Lote 2:

4.1 Não será admitida a subcontratação do objeto contratual, nos termos do item **16.10** do TR.

CLÁUSULA QUINTA – PREÇO

5.1 O Contratante pagará à Contratada os valores estimados especificados no quadro abaixo:

LOTE 01							
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor mensal unitário (R\$) A	Valor unitário para 60 meses (R\$) B = A * 60	Valor Total 60 meses (R\$) C = B * QTD
1	02.81.00.00192352-8	Solução de Conectividade Segura TIPO 01 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 500MB.	Unidade	1589			
2	02.81.00.00192353-6	Solução de Conectividade Segura TIPO 02 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 2 links (redundância) de internet banda larga com velocidade de 500MB.	Unidade	707			

3	02.81.00.00192354-4	Solução de Conectividade Segura TIPO 03 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 1GB.	Unidade	109			
4	02.81.00.00192355-2	Solução de Conectividade Segura TIPO 04 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 2 links (redundância) de internet banda larga com velocidade de 1GB.	Unidade	167			
5	02.81.00.00192356-0	Solução de Conectividade Segura TIPO 05 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários em unidades remotas que não possuem viabilidade de conexão via fibra ótica, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 1 link satélite com velocidade de 100 MB.	Unidade	149			

6	02.81.00.00192357-9	Solução de Conectividade Segura TIPO 06 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 1 link de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.	Unidade	101			
7	02.81.00.00192358-7	Solução de Conectividade Segura TIPO 07 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 500MB.	Unidade	54			
8	02.81.00.00192359-5	Solução de Conectividade Segura TIPO 08 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 500MB.	Unidade	16			

9	02.81.00.00192360-9	Solução de Conectividade Segura TIPO 09 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 1GB.	Unidade	78			
10	02.81.00.00192361-7	Solução de Conectividade Segura TIPO 10 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 1GB.	Unidade	33			
11	02.81.00.00192362-5	Solução de Conectividade Segura TIPO 11 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB.	Unidade	91			
12	02.81.00.00192363-3	Solução de Conectividade Segura TIPO 12 Solução de conectividade segura prestada em regime	Unidade	14			

		contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB e 1 link de internet banda larga com velocidade de 500MB.					
13	02.81.00.00192364-1	Solução de Conectividade Segura TIPO 13 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades com até 40 usuários e que já possuem link de internet contemplando 01 firewall de próxima geração (NGFW) com tecnologia SD-WAN.	Unidade	105			
14	02.81.00.00192365-0	Solução de Conectividade Segura TIPO 14 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades acima de 40 usuários e que já possuem link de internet contemplando 01 firewall de próxima geração (NGFW) com tecnologia SD-WAN.	Unidade	50			
15	02.81.00.00192366-8	Solução de Conectividade Segura TIPO 15 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários,	Unidade	20			

		incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN, 2 links (redundância) de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.					
16	02.81.00.00192367-6	Solução de Conectividade Segura TIPO 16 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN, 2 links (redundância) de internet banda larga com velocidade de 1GB e 1 link satélite com velocidade de 100 MB.	Unidade	16			
17	02.81.00.00192368-4	Solução de Conectividade Segura TIPO 17 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, destinada a unidades com até 05 usuários, contemplando 1 link de internet banda larga com velocidade de 200 Mbps e mecanismos de segurança providos de forma centralizada, sob gestão da PRODEB, sem a necessidade de firewall de borda dedicado na unidade.	Unidade	369			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)	

18	02.81.00.00192370-6	Serviço de Mudança de Endereço – até 300 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	137			
19	02.81.00.00192371-4	Serviço de Mudança de Endereço – acima de 300 km até 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	144			
20	02.81.00.00192372-2	Serviço de Mudança de Endereço – acima de 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	108			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor mensal unitário (R\$) A	Valor unitário para 60 meses (R\$) B = A * 60	Valor Total 60 meses (R\$) C = B * QTD

21	02.81.09.00008168-0	Solução de Operação e Monitoramento Central, prestada em regime contínuo e remunerada por valor mensal, dimensionada para atender até 500 (quinhentas) unidades de solução de conectividade segura em operação	Unidade	10			
22	02.81.09.00008169-8	Solução de Monitoramento e Relatoria De Logs Tipo I	Unidade	02			
23	02.81.00.00192944-5	Solução de Monitoramento e Relatoria De Logs Tipo II	Unidade	50			
24	02.81.00.00192945-3	Solução de Monitoramento e Relatoria De Logs Tipo III	Unidade	04			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)		Valor Total (R\$)
25	02.81.00.00192946-1	UST – Unidade de Serviços Técnicos	Unidade	5.000			
Valor Global do Lote 01:							

LOTE 02						
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)
1	02.81.00.00192373-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600E, pelo período de 12 meses	Unidade	04		
2	02.81.00.00192374-9	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 601E, pelo período de 12 meses	Unidade	04		

3	02.81.00.00192375-7	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 400F, pelo período de 12 meses	Unidade	08		
4	02.81.00.00192376-5	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200F, pelo período de 12 meses	Unidade	09		
5	02.81.00.00192377-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200E, pelo período de 12 meses	Unidade	04		
6	02.81.00.00192378-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 100F, pelo período de 12 meses	Unidade	24		
7	02.81.00.00192379-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 80F, pelo período de 12 meses	Unidade	12		
8	02.81.00.00192380-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 60F, pelo período de 12 meses	Unidade	300		

9	02.81.00.00192381-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 61F, pelo período de 12 meses	Unidade	300		
10	02.81.00.00192382-0	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 150G, pelo período de 12 meses	Unidade	04		
11	02.81.00.00192383-8	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 300G, pelo período de 12 meses	Unidade	04		
12	02.81.00.00192384-6	Serviço de Licenciamento e Atualização das Funcionalidades de Autenticação Centralizada de Usuários Marca Fortinet Modelo FortiAuthenticator 800F, pelo período de 12 meses	Unidade	04		
13	02.81.00.00192385-4	Solução De Segurança de Rede NGFW TIPO I, com licenciamento pelo período de 12 meses	Unidade	04		
14	02.81.00.00192386-2	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede - Segmentação Interna TIPO I, pelo período de 12 meses	Unidade	04		

15	02.81.00.00192947-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3700F, pelo período de 12 meses	Unidade	04		
16	02.81.00.00192948-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3301E, pelo período de 12 meses	Unidade	04		
17	02.81.00.00192949-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3000D, pelo período de 12 meses	Unidade	02		
18	02.81.00.00192950-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600F, pelo período de 12 meses	Unidade	04		
19	02.81.00.00192951-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 40F, pelo período de 12 meses	Unidade	60		
20	02.81.00.00192952-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate-VM08, pelo período de 12 meses	Unidade	02		

21	02.81.00.00192953-4	Serviço de Licenciamento e Atualização das Funcionalidades de WAF Marca Fortinet Modelo FortiWeb2000F, pelo período de 12 meses	Unidade	04		
22	02.81.00.00192954-2	Serviço de Licenciamento e Atualização das Funcionalidades de ADC Marca Fortinet Modelo FortiADC-400F, pelo período de 12 meses	Unidade	02		
23	02.80.00.00192955-0	Serviço de Licenciamento e Atualização das Funcionalidades de Gerenciador Centralizada de Dispositivos Marca Fortinet Modelo FortiManager 3000G, pelo período de 12 meses	Unidade	02		
24	02.81.00.00192956-9	Serviço de Licenciamento e Atualização das Funcionalidades de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	02		
25	02.81.00.00192957-7	Serviço de Upgrade para 50 Devices e 500 EPS de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	04		
26	02.81.00.00192958-5	Solução De Segurança de Aplicações WAF - TIPO I, com licenciamento pelo período de 12 meses	Unidade	02		
27	02.81.00.00192959-3	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF - TIPO I, pelo período de 12 meses	Unidade	02		

28	02.81.00.00192989-5	Solução De Segurança de Aplicações WAF - TIPO II, com licenciamento pelo período de 12 meses	Unidade	10		
29	02.81.00.00192990-9	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF –TIPO II, pelo período de 12 meses	Unidade	10		
30	02.81.00.00192962-3	Solução de Segurança de Aplicações WAF para Ambientes Híbridos, com licenciamento pelo período de 12 meses	Unidade	10		
31	02.81.00.00192963-1	Serviço de Licenciamento e Atualização das Funcionalidades de Solução de Segurança de Aplicações WAF para Ambientes Híbridos, pelo período de 12 meses	Unidade	10		
32	02.81.00.00192964-0	Solução de Segurança Decoy/Honeypot, com licenciamento pelo período de 12 meses	Unidade	06		
33	02.81.00.00192965-8	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança Decoy/Honeypot, pelo período de 12 meses	Unidade	06		
34	02.81.00.00192966-6	Solução de Segurança de Rede NGFW TIPO II, com licenciamento pelo período de 12 meses	Unidade	100		
35	02.81.00.00192967-4	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna TIPO II, pelo período de 12 meses	Unidade	100		
36	02.81.00.00192968-2	Solução de Segurança de Rede NGFW TIPO III, com licenciamento pelo período de 12 meses	Unidade	50		
37	02.81.00.00192969-0	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna	Unidade	50		

		TIPO III, pelo período de 12 meses				
Valor Global do Lote 02						R\$

5.1.1 Estima-se para o Contrato o valor global de R\$ ____ (____)

5.2. Nos preços contratados estão incluídos todos os custos com material de consumo, salários, encargos sociais, previdenciários, fiscais, comerciais e trabalhistas de todo o pessoal da Contratada, como também fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, tributos, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela Contratada das obrigações.

5.3 O valor do Contrato referido nesta Cláusula é meramente estimativo, dependendo os pagamentos devidos à Contratada dos quantitativos efetivamente executados.

CLÁUSULA SEXTA – PAGAMENTO

6.1 O prazo para pagamento à Contratada e as demais condições a ele referentes encontram-se definidos no **item 18** do TR, que constitui anexo deste Contrato (art. 92, incs. V e VI, da Lei Federal nº 14.133/2021).

CLÁUSULA SÉTIMA – MANUTENÇÃO DO EQUILÍBRIO ECONÔMICO FINANCEIRO DO CONTRATO

Reajustamento em sentido estrito

7.1 Os preços inicialmente contratados são fixos e irredutíveis no prazo de 1 (um) ano contado de __/__/__, **data do orçamento estimado** (art. 92, inc. V, e §3º, da Lei Federal nº 14.133/2021).

7.2 Após o interregno de 1 (um) ano, independentemente de pedido da Contratada, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do índice INPC/IBGE.

7.2.1 Na hipótese de não reajustamento dos preços pelo Contratante, o requerimento de reajuste deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação nos termos do art. 131, parágrafo único, da Lei Federal nº 14.133/2021, sob pena de preclusão.

7.3 Nos reajustamentos subsequentes ao primeiro, o interregno mínimo de 1 (um) ano será contado a partir dos efeitos financeiros do último reajuste.

7.4 Na hipótese de atraso ou não divulgação do(s) índice(s) de reajustamento, o Contratante pagará à Contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.4.1 A Contratada deverá apresentar a memória de cálculo referente ao reajustamento de preços correspondente a eventual valor remanescente.

7.5 Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

7.6 Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço no período remanescente do Contrato, por meio de termo aditivo.

7.7 O reajustamento será realizado por apostilamento, na forma do art. 136, inc. I, da Lei Federal nº 14.133/2021.

Outras causas de reequilíbrio econômico-financeiro

7.8 O reestabelecimento do equilíbrio econômico-financeiro dependerá de requerimento da Contratada quando visar recompor o preço que se tornou insuficiente, devendo ser instruído com a documentação

que comprove o desequilíbrio econômico-financeiro do Contrato.

7.8.1 O requerimento de restabelecimento do equilíbrio econômico-financeiro inicial do Contrato, nas hipóteses do art. 124, inc. II, "d", da Lei Federal nº 14.133/2021, deverá ser formulado pelo interessado no prazo máximo de 1 (um) ano do fato que o ensejou, sob pena de decadência, em consonância com o art. 211 da Lei Federal nº 10.406, de 10 de janeiro de 2002.

7.8.2 Na hipótese de contratos de fornecimento ou serviços contínuos, o requerimento de restabelecimento do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do Contrato e antes de eventual prorrogação nos termos do art. 107 da Lei Federal nº 14.133/2021, sob pena de preclusão (art. 131, parágrafo único, da Lei Federal nº 14.133/2021).

7.8.2.1 Fica convencionado que, nos casos de contrato de fornecimento ou serviços contínuos com prazo de vigência superior a 1 (um) ano, o requerimento de restabelecimento do equilíbrio econômico-financeiro do Contrato deverá observar a disposição da subcláusula 7.8.1.

7.9 O Contratante, no prazo máximo de 60 (sessenta) dias, prorrogável por igual período mediante justificativa, responderá a eventuais pedidos de manutenção do equilíbrio econômico-financeiro do Contrato apresentado pela Contratada (art. 92, inc. XI, c/c art. 123, parágrafo único, da Lei Federal nº 14.133/2021).

7.10 O processo de reestabelecimento do equilíbrio econômico-financeiro em favor do Contratante deverá ser instaurado quando possível a redução do preço ajustado para compatibilizá-lo ao valor de mercado ou quando houver diminuição, devidamente comprovada, dos preços dos insumos básicos utilizados no Contrato.

7.11 A Contratada não fará jus à recomposição do equilíbrio econômico-financeiro caso quaisquer dos riscos por ela assumidos no Contrato venham a se materializar (art. 124, inc. II, "d", parte final, da Lei Federal nº 14.133/2021);

7.12 No caso de contratações de obras e serviços de engenharia, a hipótese de que trata a subcláusula 7.8.1 abrange as situações em que a execução contratual seja obstada pelo atraso na conclusão de procedimentos de desapropriação, desocupação, servidão administrativa ou licenciamento ambiental, por circunstâncias alheias à Contratada (art. 124, §2º, da Lei Federal nº 14.133/2021).

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE E DA CONTRATADA

Obrigações do Contratante

8.1 O Contratante, além das determinações contidas no TR e demais componentes, bem como daquelas decorrentes de lei, obriga-se a:

- a) exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com este Contrato e seus anexos, fornecendo por escrito as informações necessárias para a execução do objeto contratado;
- b) receber o objeto no prazo e condições estabelecidas no TR;
- c) acompanhar e fiscalizar a execução do Contrato e o cumprimento das obrigações pela Contratada;
- d) intimar a Contratada, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto do Contrato, para que seja por ela substituído, reparado ou corrigido, no total ou em parte, às suas expensas, no prazo indicado, certificando-se de que as soluções propostas pela Contratada são as mais adequadas;
- e) comunicar-se com a Contratada para emissão de nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) relativamente à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei Federal nº 14.133/2021;
- f) efetuar o pagamento à Contratada do valor correspondente à execução do objeto, conforme prazo, forma e condições estabelecidos no TR;
- g) aplicar à Contratada as sanções previstas em lei e neste Contrato;
- h) explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato apresentadas pela Contratada, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, no prazo definido na subcláusula 8.1.1;
- i) responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro apresentados pela Contratada no prazo definido na subcláusula 7.9;
- j) intimar os emitentes das garantias relativamente ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, §4º, da Lei Federal nº 14.133/2021);
- k) assegurar-se, na hipótese de execução do objeto contratado em suas dependências ou em local por ele designado, que o ambiente de trabalho, inclusive seus equipamentos e instalações, apresentem condições adequadas ao cumprimento, pela Contratada, das normas de segurança e saúde no trabalho;

8.1.1 O Contratante, no prazo de () dias, a contar da data do protocolo do(s) requerimento(s) relacionado(s) à execução do Contrato, decidirá sobre todas as solicitações e

reclamações apresentadas pela Contratada, admitida a prorrogação motivada do prazo, por igual período (art. 123 da Lei Federal nº 14.133/2021).

8.1.2 Além das determinações acima descritas, o Contratante deverá atender às obrigações específicas nos itens **24, 25.2 (Lote 1 – SAEB), 25.4 (Lote 1 – Demais órgãos)**

Obrigações da Contratada

8.2 A Contratada deve cumprir todas as obrigações constantes neste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações decorrentes de lei e aquelas a seguir dispostas:

- a) designar de sua estrutura administrativa um preposto permanentemente responsável pela perfeita execução do Contrato, inclusive para atendimento de emergência, servindo de interlocutor e canal de comunicação entre as partes, observado o art. 118 da Lei Federal nº 14.133/2021, cuja designação ou manutenção poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, hipótese em que a Contratada designará outro profissional para o exercício da atividade;
- b) atender às determinações regulares emitidas pelo Contratante e prestar o(s) esclarecimento(s) ou informação(ões) por ele solicitado(s) (art. 137, inc. II, da Lei Federal nº 14.133/2021);
- c) reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo Contratante, os bens e serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
- d) responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, nos termos das normas de regência, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;
- e) não contratar, durante a vigência do Contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do Contratante ou do fiscal ou gestor do Contrato, nos termos do art. 48, parágrafo único, da Lei Federal nº 14.133/2021;
- f) quando não for possível a verificação da regularidade no Cadastro de Fornecedores, entregar ao setor responsável pela fiscalização do Contrato, junto com a nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda estadual, municipal ou distrital do domicílio ou sede da Contratada; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;
- g) manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação ou no procedimento de contratação direta;
- h) prestar todo esclarecimento ou informação solicitados pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do objeto;
- i) executar o objeto sem solução de continuidade durante todo o prazo da vigência do Contrato e comunicar ao Contratante qualquer anormalidade ou acidente que interfira no bom andamento do Contrato;
- j) paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;
- k) promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do Contrato;
- l) conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local da execução do objeto e nas melhores condições de segurança, higiene e disciplina;
- m) reparar, repor ou restituir, nas mesmas condições e especificações, dentro do prazo determinado pelo Contratante, os equipamentos e utensílios eventualmente recebidos para uso nos serviços objeto deste contrato, deixando-os em perfeita condição de funcionamento;
- n) assegurar a seus trabalhadores ambiente de trabalho em condições adequadas ao cumprimento às normas de saúde, segurança e bem estar no trabalho e fazer com que seus empregados as respeitem, bem como atentar para as regras de cortesia no local onde serão executados os serviços;
- o) responsabilizar-se pelo cumprimento das obrigações trabalhistas, sociais, previdenciárias, tributárias, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;
- p) submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do TR e/ou Projeto Básico;
- q) cumprir, durante todo o período de execução do Contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas

de cargos previstas em outras normas específicas, devendo, sempre que solicitado pelo Contratante, indicar os empregados que preencherem as vagas correspondentes (arts. 92, inc. XVIII, e 116 da Lei Federal nº 14.133/2021);

r) atender as obrigações concernentes à aprendizagem de que trata o art. 429 do Decreto-Lei nº 5.452/1943 (Consolidação das Leis do Trabalho - CLT), Lei nº 14.395/2021, e normas regulamentares, em especial:

1) quando se tratar da contratação de serviços, recrutar, preferencialmente, como aprendizes, os estudantes indicados no art. 42 da Lei nº 14.395/2021, no percentual mínimo de 20% (vinte por cento) do quadro de aprendizes da Contratada.

1.1) na hipótese do item 1, a Contratada deverá apresentar ao fiscal ou responsável pela gestão e acompanhamento do Contrato, no prazo de até 05 (cinco) dias úteis, contado do início efetivo da execução do objeto, a lista completa dos aprendizes, indicando aqueles selecionados no banco de dados de que trata a Lei nº 14.395/2021, devendo justificar, perante o Contratante, a eventual impossibilidade de seu cumprimento.

s) guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato;

t) arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, inc. II, "d", da Lei Federal nº 14.133/2021;

u) observar a legislação federal, estadual e municipal, relativa ao objeto do Contrato, bem como as normas internas do Contratante;

v) alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste Contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

x) não permitir a utilização de qualquer trabalho do menor de 16 (dezesesseis) anos, exceto na condição de aprendiz para os maiores de 14 (quatorze) anos, nem permitir a utilização do trabalho do menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre;

y) providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes, necessários à execução do Contrato, arcando com os custos para sua obtenção;

w) efetuar pontualmente o pagamento de tributos que incidam ou venham a incidir sobre as suas atividades e/ou sobre a execução do presente Contrato;

z) emitir nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) de acordo com a legislação, contendo descrição dos bens, obras e/ou serviços, com o valor exato dimensionado pela fiscalização, indicando, conforme o caso, sua quantidade, preço unitário e valor total;

aa) realizar os serviços de manutenção e assistência técnica conforme prescrições do TR;

bb) fornecer as instalações, aparelhamento e pessoal técnico exigidos na licitação ou no procedimento de contratação direta;

cc) alocar, durante todo o período de execução do objeto, profissional, devidamente registrado no conselho profissional competente, quando for o caso, detentor de atestado de responsabilidade técnica e a equipe técnica mínima exigida no TR, admitindo-se a sua substituição por profissionais de experiência equivalente ou superior, desde que aprovada pelo Contratante;

dd) responder por quaisquer compromissos assumidos com terceiros, bem como por qualquer dano causado a terceiros em decorrência de ato próprio, de seus empregados, prepostos ou subordinados;

ee) promover, por sua conta e risco, transporte de bens;

ff) executar, quando for o caso, a montagem dos equipamentos, de acordo com as especificações e/ou normas exigidas, utilizando ferramentas apropriadas e dispondo de infraestrutura e equipe técnica necessárias à sua execução;

gg) ressarcir o Contratante pelos danos decorrentes de paralisação ou interrupção da execução do objeto contratado;

hh) realizar, quando exigido no TR, a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo ser exigida, inclusive, a capacitação dos técnicos do Contratante ou da nova empresa que continuará a execução dos serviços.

ii) tratando-se de obras, serviços e fornecimento de grande vulto, implantar Programa de Integridade, na forma do Decreto nº 23.356, de 17 de janeiro de 2025;

jj) providenciar o cadastramento de seu representante legal ou procurador no site www.comprasnet.ba.gov.br ou outro que venha a substituí-lo, para a prática de atos através do Sistema Eletrônico de Informações – SEI;

kk) manter atualizados os seus dados cadastrais, com a apresentação de documentos comprobatórios de mudança de endereços, inclusive eletrônicos (e-mail), telefones, composição societária, endereço dos sócios, contratos sociais e alterações;

ll) atender às obrigações de que tratam os Anexos deste Contrato;

mm) entregar o objeto de acordo com as especificações técnicas constantes do TR e no presente Contrato, nos locais, dias, turnos e horários determinados, acompanhado do manual do usuário, com uma versão em português, e da relação da rede de assistência técnica autorizada, se houver.

8.2.1 Além das determinações acima descritas, a Contratada deverá atender às obrigações específicas previstas nos itens **22, 23, 25.1 (Lote 1), 28 (Lote 1) e 29 do TR.**

8.3 A Matriz de Risco constitui parte integrante deste Contrato, independentemente de transcrição, na forma do Anexo deste Contrato.

8.3.1 A Contratada não é responsável pelos riscos relacionados ao objeto do ajuste cuja responsabilidade tenha sido atribuída ao Contratante na Matriz de Risco, sem prejuízo da responsabilidade deste pelo cumprimento das obrigações elencadas na subcláusula 8.1.

8.3.2 A Contratada é integral e exclusivamente responsável por todos os riscos relacionados ao objeto do ajuste a ela atribuídos na Matriz de Risco, sem prejuízo da sua responsabilidade pelo cumprimento das obrigações elencadas na subcláusula 8.2.

CLÁUSULA NONA – GARANTIA DA CONTRATAÇÃO

9.1 As disposições sobre a garantia da contratação estão disciplinadas no **item 32 do TR.**

CLÁUSULA DÉCIMA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

10.1 Constituem infrações administrativas para os fins deste Contrato, as condutas tipificadas no art. 155 da Lei Federal nº 14.133/2021.

10.2 Serão aplicadas à Contratada que incorrer nas infrações tipificadas no art. 155 da Lei Federal nº 14.133/2021, as sanções previstas no art. 156 da mesma norma, observados os arts. 48 e 49 da Lei nº 14.634/2023 e a disciplina constante no Decreto nº 23.113/2024.

10.3 No que concerne à multa, será observado o disposto no subitem 10.14.

10.4 A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante, observado o disposto na Lei nº 12.209, de 20 de abril de 2011 (art. 156, §9º, da Lei Federal nº 14.133/2021).

10.5 Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei Federal nº 14.133/2021).

10.6 A apuração das infrações administrativas será realizada em processo administrativo sancionatório, conforme rito estabelecido nos arts. 51 e 52 da Lei nº 14.634/2023, com a observância das garantias da ampla defesa e do contraditório, na forma do Decreto nº 23.113/2024.

10.6.1 Será admitida medida cautelar destinada a garantir o resultado útil do processo administrativo sancionatório, de forma antecedente ou incidental à sua instauração, inclusive a retenção provisória do valor correspondente à estimativa da sanção de multa (art. 50, §2º, da Lei nº 14.634/2023).

10.6.2 O valor da retenção provisória a que se refere a subcláusula anterior não poderá exceder o limite máximo estabelecido no art. 156, §3º, da Lei Federal nº 14.133/2021 (art. 50, §3º, da Lei nº 14.634/2023).

10.7 A apuração de infrações sujeitas exclusivamente à sanção de advertência ou de multa, isoladas ou cumuladas entre si, será realizada em processo sancionatório simplificado (art. 51 da Lei nº 14.634/2023).

10.7.1 Precederá a abertura do processo sancionatório simplificado a intimação do interessado a fim de que tenha ciência da imputação, observada a disciplina do art. 28 do Decreto nº 23.113/2024.

10.7.1.1 O ato de intimação deverá conter a descrição dos fatos ilícitos imputados, o enquadramento jurídico, a sanção aplicável e, no caso de multa, o respectivo cálculo.

10.7.1.2 Acompanhará o ato de intimação o termo de anuência que poderá ser firmado pelo interessado, caso manifeste a concordância com a imputação e com a sanção aplicável.

10.7.1.3 Assinado o termo de anuência no prazo assinalado, será promovida a aplicação da sanção cabível, procedendo-se aos devidos registros, encerrando-se o procedimento.

10.7.1.3.1 No caso de multa, o procedimento será encerrado após o seu efetivo recolhimento.

10.7.1.4 Caso o interessado não manifeste a concordância expressa com os termos da imputação, será promovida a abertura do processo sancionatório simplificado.

10.8. A apuração de conduta infrativa sujeita à sanção de impedimento de licitar e contratar ou de declaração de inidoneidade para licitar ou contratar, será realizada em processo de responsabilização (art. 52 da Lei nº 14.634/2023).

10.8.1. As sanções de impedimento de licitar e contratar ou de declaração de inidoneidade para licitar ou contratar poderão ser atenuadas ou comutadas mediante a celebração de Termo de Transação Administrativa (TTA), observados os requisitos e condições estabelecidos em Regulamento específico (art. 55 do Decreto nº 23.113/2024).

- 10.9 Na aplicação das sanções serão considerados (art. 156, §1º, da Lei Federal nº 14.133/2021):
- a) a natureza e a gravidade da infração cometida;
 - b) as peculiaridades do caso concreto;
 - c) as circunstâncias agravantes ou atenuantes;
 - d) os danos que dela provierem para o Contratante;
 - e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- 10.10 Os atos previstos como infrações administrativas na Lei Federal nº 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei Federal nº 12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei (art. 159 da Lei Federal nº 14.133/2021 e art. 47, §3º, da Lei nº 14.634/2023).
- 10.11 A personalidade jurídica da Contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos em lei e neste Contrato ou para provocar confusão patrimonial (art. 160 da Lei Federal nº 14.133/2021 e art. 57 da Lei nº 14.634/2023).
- 10.11.1 Com a desconsideração da personalidade jurídica, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a Contratada.
- 10.11.2 Em todos os casos de desconsideração da personalidade jurídica deverão ser observados o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.
- 10.12 O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal (art. 161 da Lei Federal nº 14.133/2021 e art. 55, §1º, da Lei nº 14.634/2023).
- 10.13 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei Federal nº 14.133/2021, conforme art. 60 da Lei nº 14.634/2023 e a disciplina prevista no Decreto nº 23.113/2024.
- 10.14 A sanção de multa observará as seguintes disposições:
- 10.14.1 Multa Compensatória
- 10.14.1.1 A multa compensatória, em caso de descumprimento total da **obrigação principal**, incidente sobre o valor global do contrato, será de: 15% (quinze por cento) (art. 8º, *caput*, e §1º do Decreto nº 23.313/2024).
- 10.14.1.1.1 Caso o cumprimento da **obrigação principal**, uma vez iniciado, seja descontinuado, a multa compensatória incidirá sobre a diferença entre o valor global do contrato e o valor da parte do fornecimento ou do serviço já realizado (art. 8º, §2º do Decreto nº 23.313/2024).
- 10.14.1.2 A multa compensatória, no caso de descumprimento de **obrigação acessória**, incidente sobre o valor do contrato, será de: 15% (quinze por cento) (art. 8º, §3º, do Decreto nº 23.313/2024).
- 10.14.2 Multa Moratória
- 10.14.2.1 O atraso injustificado na execução do contrato sujeitará o contratado a multa de mora.
- 10.14.2.2 No caso de **obrigação principal**, a multa de mora diária, incidente sobre o valor da obrigação descumprida ou da estimativa arbitrada de seu custo, será de: 0,1% (um décimo por cento) (art. 9º, §1º, do Decreto nº 23.313/2024).
- 10.14.2.3 No caso de **obrigação acessória**, a multa de mora diária, incidente sobre o valor da obrigação descumprida ou da estimativa arbitrada de seu custo, será de: 0,1% (um décimo por cento).
- 10.14.2.4 O atraso injustificado do prazo fixado para **apresentação, suplementação ou reposição de garantia contratual** ensejará a aplicação de multa moratória diária de 0,1% (um décimo por cento), incidente sobre o valor da garantia contratual (art. 9º, §2º, do Decreto nº 23.313/2024).
- 10.14.2.4.1 A multa moratória não poderá superar o valor da própria garantia contratual.
- 10.14.2.5 A aplicação de multa de mora não impedirá que a Administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções previstas na Lei nº 14.133/2021 (art. 9º, §3º, do Decreto nº 23.313/2024).
- 10.14.2.6 Se o cálculo da multa moratória atingir o patamar correspondente ao valor máximo da multa compensatória, além da conversão em compensatória e aplicação das demais sanções

previstas em lei, o recebimento do objeto deverá ser recusado, salvo justificativa escrita devidamente fundamentada (art. 9º, §4º, do Decreto nº 23.313/2024).

CLÁUSULA DÉCIMA PRIMEIRA – EXTINÇÃO CONTRATUAL

11.1 O Contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes.

11.1.1 O Contrato pode ser extinto antes do prazo nele fixado, sem ônus para o Contratante, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o Contrato não mais lhe oferece vantagem (art. 106, inc. III, da Lei Federal nº 14.133/2021).

11.1.1.1 Na hipótese de que trata a subcláusula 11.1.1, a extinção ocorrerá na próxima data de aniversário do Contrato, condicionada à intimação da Contratada sobre a não continuidade do pacto com, no mínimo, 2 (dois) meses de antecedência da referida data (art. 106, §1º, da Lei Federal nº 14.133/2021).

11.1.1.1.1 Caso a intimação de que trata a subcláusula 11.1.1 ocorra com menos de 2 (dois) meses da data de aniversário do Contrato, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

11.2. O Contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no art. 137 da Lei Federal nº 14.133/2021, assegurados o contraditório e a ampla defesa.

11.2.1. A extinção do contrato poderá ser:

- a) determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta (arts. 138, inc. I, e 139 da Lei Federal nº 14.133/2021);
- b) consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração (art. 138, inc. II, da Lei Federal nº 14.133/2021);
- c) determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial (art. 138, inc. III, da Lei Federal nº 14.133/2021).

11.2.2. A alteração social, da finalidade ou da estrutura da empresa Contratada não ensejará a extinção contratual se não restringir sua capacidade de concluir o Contrato (art. 137, inc. III, da Lei Federal nº 14.133/2021).

11.2.2.1. Se a alteração de que trata a subcláusula 11.2.2 implicar mudança da pessoa jurídica Contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

11.2.3. O Contrato será extinto caso se constate que a Contratada mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou da entidade Contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do Contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inc. IV, da Lei Federal nº 14.133/2021).

11.3 O termo de extinção, sempre que possível, será precedido de:

- a) balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;
- b) relação dos pagamentos já efetuados e ainda devidos;
- c) indenizações e multas.

11.4 A extinção do Contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, observada a Cláusula Sétima deste Contrato, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131 da Lei Federal nº 14.133/2021).

CLÁUSULA DÉCIMA SEGUNDA – DOTAÇÃO ORÇAMENTÁRIA

12.1 As despesas para o pagamento do presente Contrato correrão à conta de recursos da Dotação Orçamentária a seguir especificada (art. 92, inc. VIII, da Lei Federal nº 14.133/2021):

Unidade FIPLAN	Função	Subfunção	Programa	P/A/OE
Região/planejamento	Natureza da despesa	Destinação do recurso	Tipo de recurso orçamentário	

12.2 A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e a liberação dos créditos correspondentes, mediante apostilamento.

CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1 Eventuais alterações contratuais se regerão pela disciplina dos arts. 124 e seguintes da Lei Federal nº 14.133/2021.

13.2 A Contratada é obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato que se fizerem nas obras, nos serviços ou nas compras, e, de até 50% (cinquenta por cento), no caso de reforma de edifício ou de equipamento (art. 125 da Lei Federal nº 14.133/2021).

13.3 As alterações unilaterais não poderão transfigurar o objeto da contratação (art. 126 da Lei Federal nº 14.133/2021).

13.4 Caso o Contrato não contemple preços unitários para obras ou serviços cujo aditamento se fizer necessário, esses serão fixados por meio da aplicação da relação geral entre os valores da proposta e o do orçamento-base da Administração sobre os preços referenciais ou de mercado vigentes na data do aditamento, respeitados os limites estabelecidos na subcláusula 13.2 (art. 127 da Lei Federal nº 14.133/2021).

13.5 Nas alterações contratuais para supressão de obras, bens ou serviços, se a Contratada já houver adquirido os materiais e os colocado no local dos trabalhos, estes deverão ser pagos pela Administração pelos custos de aquisição regularmente comprovados e monetariamente reajustados, podendo caber indenização por outros danos eventualmente decorrentes da supressão, desde que regularmente comprovados (art. 129 da Lei Federal nº 14.133/2021).

13.6 Caso haja alteração unilateral do Contrato que aumente ou diminua os encargos da Contratada, a Administração deverá restabelecer, no mesmo termo aditivo, o equilíbrio econômico-financeiro inicial (art. 130 da Lei Federal nº 14.133/2021).

13.7 Os preços contratados serão alterados, para mais ou para menos, conforme o caso, se houver, após a data da apresentação da proposta, criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços contratados (art. 134 da Lei Federal nº 14.133/2021).

13.8 Nas contratações de obras e serviços de engenharia, a diferença percentual entre o valor global do Contrato e o preço global de referência não poderá ser reduzida em favor da Contratada em decorrência de aditamentos que modifiquem a planilha orçamentária (art. 128 da Lei Federal nº 14.133/2021).

13.9 As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação do órgão de assessoramento jurídico do Contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei Federal nº 14.133/2021).

13.10. Registros que não caracterizam alteração do Contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, conforme art. 136 da Lei Federal nº 14.133/2021.

CLÁUSULA DÉCIMA QUARTA – PUBLICAÇÃO

14.1. Incumbirá ao Contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei Federal nº 14.133/2021.

CLÁUSULA DÉCIMA QUINTA – COMUNICAÇÃO ELETRÔNICA

15.1. Fica pactuado que os atos de comunicação processual com a Contratada poderão ser realizados por meio eletrônico, na forma da Lei nº 12.209/2011 e do Decreto nº 15.805, de 30 de dezembro de 2014.

15.1.1. A Contratada deverá manter atualizado o endereço eletrônico cadastrado no Sistema Eletrônico de Informações - SEI, para efeito do recebimento de notificação e intimação de atos processuais, conforme Decreto nº 17.983, de 24 de outubro de 2017, devendo atender às convocações da Administração para a prática de atos nos prazos indicados.

CLÁUSULA DÉCIMA SEXTA - OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

16.1 As partes se comprometem a cumprir a Lei Federal nº 13.709/2018 (Lei de Proteção de Dados Pessoais - LGPD), bem como regras e regulamentos que lhe forem aplicáveis e que tenham por objeto os dados pessoais tratados no âmbito do objeto contratado.

16.2 A Contratada deverá utilizar os dados pessoais recebidos em função do objeto do Contrato somente para a finalidade pactuada, não podendo, em caso algum, utilizar esses dados pessoais para finalidade distinta, sob pena de extinção imediata da contratação.

16.3 A Contratada se obriga a não armazenar, arquivar, reproduzir, transmitir, distribuir, transferir ou de qualquer forma compartilhar os dados pessoais disponibilizados pelo Contratante com terceiros, salvo nas hipóteses legalmente previstas.

16.4 Em caso de incidente de vazamento de dados pessoais, a Contratada deverá enviar comunicação ao Contratante, por escrito, no prazo máximo de 24 (vinte e quatro) horas contado a partir da ciência do vazamento, contendo, no mínimo, as seguintes informações: a) data e hora do incidente; b) data e hora da ciência pela Contratada; c) relação dos tipos de dados afetados pelo incidente; d) relação de titulares afetados pelo incidente; e e) indicação de medidas que estiverem sendo tomadas para sanar e mitigar o incidente, bem como para reparar eventuais danos e evitar novos incidentes.

16.5 O Contratante deverá ser informado no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pela Contratada.

16.6 A Contratada deverá exigir de suboperadores e subcontratados o cumprimento dos deveres desta Cláusula, permanecendo integralmente responsável por garantir sua observância.

16.7 Encerrado o tratamento dos dados nos termos do art. 15 da LGPD, é dever da Contratada eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

16.8 A Contratada deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações sobre os dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

16.9 Em caso de descumprimento de qualquer obrigação prevista nesta Cláusula, a Contratada ficará sujeita à integral responsabilização, inclusive por perdas e danos, aplicação das sanções cabíveis e da extinção do Contrato.

CLÁUSULA DÉCIMA SÉTIMA – DISPOSIÇÕES GERAIS

17.1 Constatada irregularidade no procedimento licitatório, de contratação direta ou na execução contratual, caso não seja possível o saneamento, a decisão sobre a suspensão da execução ou sobre a declaração de nulidade do Contrato observará o disposto no art. 147 da Lei Federal nº 14.133/2021.

17.2 O Contratante não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do Contrato.

17.3 Os casos omissos serão dirimidos pelo Contratante, segundo as disposições contidas na Lei Federal nº 14.133/2021, na Lei nº 14.634/2023 e demais normas aplicáveis.

17.4 Na contagem dos prazos estabelecidos neste Contrato, será observado o art. 183 da Lei Federal nº 14.133/2021 e o art. 67 da Lei nº 14.634/2023.

CLÁUSULA DÉCIMA OITAVA – FORO

18.1 As partes elegem o Foro da Cidade do Salvador, Estado da Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para solucionar quaisquer dúvidas oriundas deste instrumento que não puderem ser dirimidas por quaisquer dos meios alternativos de resolução de controvérsias de que trata a Lei Federal nº 14.133/2021.

[Local], [dia] de [mês] de [ano].

Representante legal do Contratante

Representante legal da Contratada

TESTEMUNHAS:

ANEXO IV – MODELO DE DECLARAÇÃO DE ENQUADRAMENTO (LEI COMPLEMENTAR Nº 123/06), NOS TERMOS DO ART. 1º, §3º DO RLC DA PRODEB

[EXCLUSIVA PARA MICROEMPRESA E EMPRESA DE PEQUENO PORTE]

Modalidade de Licitação	Número

Para os efeitos do tratamento diferenciado da Lei Complementar nº 123/06, declaramos:

que estamos enquadrados, na data designada para o início da sessão pública da licitação, na condição
() **de microempresa** **[ou]** () **de empresa de pequeno porte**
e que não estamos incursos nas vedações a que se reporta o §4º do art. 3º da Lei Complementar nº 123/06.

Declaramos ainda que, no ano calendário de realização da presente licitação, não celebramos contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

Salvador, ____ de _____ de 20__.

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

ANEXO V – MODELO DE DECLARAÇÃO UNIFICADA

Modalidade de Licitação	Número

[Identificação completa do representante da licitante], como representante devidamente constituído de **[Identificação completa da licitante]**, doravante denominada LICITANTE, para fins de participação no certame licitatório acima identificado, declaro, sob as penas da lei, que:

- a) cumpre plenamente os requisitos de habilitação definidos neste Edital e seus anexos;
- b) não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do art. 7º, XXXIII, da Constituição Federal;
- c) que todos os custos previstos na nossa proposta estão coerentes com o mercado, o que implica na viabilidade de nossa proposta e sua exequibilidade;
- d) que não foi declarada inidônea por ato da Administração Pública;
- e) que minhas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas;
- f) que para fins do disposto no art. 116 da Lei Federal n.º 14.133/21, durante a execução do contrato, cumprirá a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas;
- g) que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

Salvador ____ de _____ de 20__.

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

ANEXO VI – MODELO DE PROCURAÇÃO

Modalidade de Licitação	Número

Através do presente instrumento, nomeamos e constituímos o(a) Senhor(a), (nacionalidade, estado civil, profissão), portador do Registro de Identidade nº, expedido pela, devidamente inscrito no Cadastro de Pessoas Físicas do Ministério da Fazenda, sob o nº, residente à rua, nº como nosso mandatário, a quem outorgamos amplos poderes para praticar todos os atos relativos ao procedimento licitatório indicado acima, conferindo-lhe poderes para:

(apresentar proposta de preços, interpor recursos e desistir deles, contra-arrazoar, assinar contratos, negociar preços e demais condições, confessar, firmar compromissos ou acordos, receber e dar quitação e praticar todos os demais atos pertinentes ao certame etc).

Salvador ____ de _____ de 20__.

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

ANEXO VII – MODELO DE PETIÇÃO DE IMPUGNAÇÃO/RECURSO

I. Identificação completa: razão social, CNPJ, endereço e nome, RG e CPF do representante legal:

II. Órgão/entidade e setor licitante:

III. Modalidade/número de ordem:

IV. Proc. Administrativo nº:

V. Finalidade da licitação/objeto:

VI. Dispositivo(s) ou ato(s) questionado(s): (Transcrever)

VII. Razões da impugnação/recurso:

...

Salvador ____ de _____ de 20__.

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

ANEXO VIII – MODELO DE PROVA DE QUALIFICAÇÃO TÉCNICA

COMPROVAÇÃO DE APTIDÃO PARA O DESEMPENHO

Modalidade de Licitação	Número

Declaramos, para fins de habilitação em processo licitatório, que a empresa
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, CNPJ XXXXXXXXXXXXXXXX, com endereço na
XXXXXXXXXXXXXXXXXXXXXXXXXXXX, prestou serviço de xxxxxxxxxxxxxxxx, atendendo integralmente as
especificações contratadas, inexistindo, até a presente data, registros negativos que comprometam a
prestação.

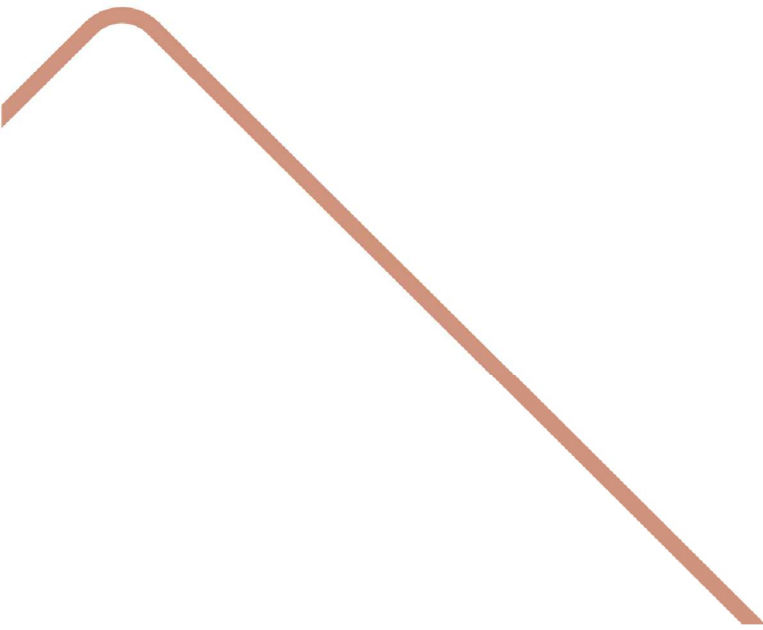
Especificação	Quantitativo	Prazo de execução

Salvador ____ de _____ de 20__.

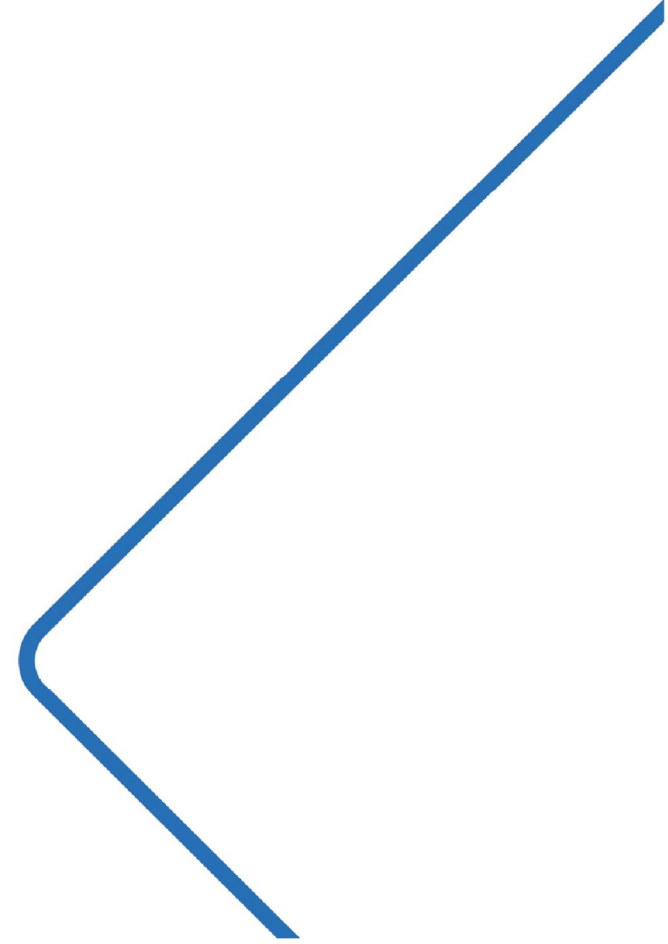
NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

Contratação de Serviços de Solução de Conectividade Segura e Soluções de Segurança da
Informação e Cibersegurança

Termo de Referência (TR)



DTC Diretoria de Infraestrutura Tecnológica e Conectividade



TERMO DE REFERÊNCIA

I. DO OBJETO

1. OBJETO DA LICITAÇÃO

1.1. Implantação de sistema de registro de preços, objetivando a formalização de ata com vencedor do certame, visando a contratação de empresa especializada em solução de conectividade segura, incluindo proteção de borda, firewall de próxima geração, links de internet e solução de operação e monitoramento central, pelo período de 60 meses e soluções de segurança da informação e cibersegurança, compreendendo licenciamento, atualização, garantia e demais serviços associados, pelo período de 12 meses, conforme abaixo:

1.1.1. LOTE 01: Solução de conectividade segura, incluindo proteção de borda, firewall de próxima geração (NGFW) com tecnologia SD-WAN, links de internet e Solução de Operação e Monitoramento Central, pelo período de 60 meses; Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço, conforme especificações técnicas detalhadas neste Termo de Referência.

1.1.2. LOTE 02: Soluções de segurança da informação e cibersegurança, compreendendo equipamentos de firewall, licenciamento, atualização, garantia e serviços de upgrade, voltados à proteção dos ambientes tecnológicos, das comunicações de dados e das aplicações corporativas dos órgãos e entidades do Poder Executivo Estadual, pelo período de 12 meses, conforme especificações técnicas detalhadas neste Termo de Referência.

1.2. Considerando que o objeto que se pretende contratar pode ser descrito de forma objetiva, possui características comuns e usuais disponíveis no mercado de Tecnologia da Informação e Comunicação - TIC, cujos padrões de desempenho e de qualidade são objetivamente definidos na especificação deste termo de referência, o mesmo pode ser enquadrado como de natureza comum.

2. JUSTIFICATIVA DA CONTRATAÇÃO

2.1. Lote 01

A contratação ora proposta tem por objetivo assegurar a continuidade, a estabilidade e a segurança dos serviços de conectividade que compõem a Rede Governo, infraestrutura esta de caráter estratégico e indispensável ao funcionamento da Administração Pública do Estado da Bahia e à prestação de serviços essenciais à população.

A Rede Governo é o alicerce tecnológico que sustenta a operação dos sistemas corporativos, a integração entre os órgãos e a disponibilização de serviços digitais ao cidadão, sendo fundamental para a execução eficiente das políticas públicas nas áreas de saúde, segurança, educação e demais serviços essenciais. Qualquer indisponibilidade ou limitação dessa infraestrutura impacta diretamente a capacidade do Estado de atender à sociedade de forma ágil, segura e contínua.

Atualmente, a infraestrutura da Rede Governo é composta por duas redes complementares: a Infovia Digital da Bahia, que atende a capital e região metropolitana, e a Rede Governo, que atende as unidades administrativas distribuídas pelo interior do Estado. A Rede Governo, estruturada por meio da RG IV, opera com contratos descentralizados firmados a partir de atas de registro de preços, contemplando múltiplos fornecedores para serviços de conectividade e um fornecedor distinto para a solução integrada de segurança da informação. **Esse modelo fragmentado tem gerado dificuldades operacionais relevantes, como a necessidade de interlocução simultânea com diversos prestadores.** Além da complexidade operacional, soma-se a proximidade do término da vigência dos contratos da RG IV.

A eventual interrupção desses serviços teria impactos imediatos e generalizados sobre a atuação do Estado, afetando atividades finalísticas e administrativas sensíveis, bem como o atendimento direto ao cidadão.

Diante desse contexto, a presente contratação foi planejada para viabilizar uma transição ordenada para a RG V, por meio da adoção de uma solução integrada de conectividade segura, capaz de operar em regime de disponibilidade contínua, com mecanismos avançados de monitoramento e resposta a incidentes. Essa medida assegura a preservação da governança centralizada da Rede Governo, a mitigação dos riscos operacionais e contratuais identificados e a observância dos princípios da continuidade, da eficiência e da supremacia do interesse público.

Ressaltamos ainda que a atuação da PRODEB na fase de planejamento contribuiu para alinhar as contratações de TIC às boas práticas e aos padrões tecnológicos do Estado, reduzindo riscos e assegurando maior aderência às diretrizes consolidadas.

Nesse sentido, o Termo de Cooperação Técnica nº 002/2026 (doc. nº 00132015637) reforça o modelo cooperativo voltado à oferta de soluções tecnológicas padronizadas, seguras e adequadas às necessidades da Administração Pública Estadual, consolidando e sistematizando práticas que já vinham sendo realizadas de forma exitosa em experiências anteriores entre a SAEB e a PRODEB.

2.1.1 Base Implantada

A PRODEB possui em sua infraestrutura uma solução de Segurança da Informação composta por Next Generation Firewalls, Relatoria, Gerenciamento Centralizado, Autenticação Centralizada, Gerenciador de eventos de Segurança e Acesso Wireless Seguro que já atende as redes IDB (Infovia Digital da Bahia) e a Rede Governo IV. Esta solução é composta pelos seguintes equipamentos:

Produto	Descrição	Part Number
FortiManager 3900E	Solução de Gerência Centralizada	FMG-3900E
FortiAnalyzer 3500F	Solução de Logs e Relatoria	FAZ-3500F
FortiAnalyzer 2000E	Solução de Logs e Relatoria	FAZ-2000E
FortiAuthenticator 3000E	Solução de Autenticação	FAC-3000E
Fortigate 3000D	Solução de Next Generation Firewall	FG-3000D
Fortigate 51E (IDB)	Solução de Next Generation Firewall	FG-51E
Forti SIEM	Monitoramento, correlação de eventos e gestão de logs	FSM

Tabela 01 – Estrutura de Segurança.

Considerando o cenário atualmente existente, a adoção de solução compatível com essa base instalada mostra-se imprescindível para garantir a continuidade operacional, a padronização tecnológica, a eficiência na gestão, bem como a mitigação de riscos associados à descontinuidade, substituições abruptas ou aumento da complexidade de operação.

Desta forma a solução ofertada para os dispositivos de segurança devem ter todas as suas funcionalidades compatíveis com os equipamentos descritos na tabela acima, permitindo assim gerenciar, monitorar, coletar logs, autenticar e garantir a total interoperabilidade entre eles, mesmo após atualizações.

Caso a solução ofertada não seja compatível com os equipamentos atualmente utilizados pela CONTRATANTE, a licitante vencedora deverá fornecer, às suas expensas, equipamentos de Next Generation Firewalls, solução de Relatoria, Gerenciamento Centralizado, Autenticação Centralizada e Gerenciador de Eventos de Segurança, em quantidade equivalente e com desempenho mínimo igual ou superior aos equipamentos existentes.

Os referidos equipamentos deverão atender integralmente às especificações descritas neste encarte e ser entregues e devidamente instalados no ambiente do Gestor Técnico — Data Center da PRODEB, localizado no Centro Administrativo da Bahia (CAB), em Salvador/BA — no prazo máximo de até 60 (sessenta) dias corridos, a contar da assinatura do contrato.

2.2. Lote 02

A contratação ora proposta tem por finalidade assegurar a continuidade e a eficácia das soluções de segurança da informação que sustentam o ambiente tecnológico do Poder Executivo Estadual, em conformidade com o modelo institucional vigente. Essas soluções, que incluem equipamentos de segurança de rede do tipo Next Generation Firewall (NGFW) e mecanismos correlatos de autenticação centralizada, auditoria e correlação de eventos, são elementos críticos para a proteção do tráfego de dados, garantindo a confidencialidade, integridade e disponibilidade das informações corporativas.

Os ativos atualmente em operação foram previamente adquiridos e encontram-se instalados em unidades administrativas e ambientes centrais, desempenhando papel essencial na prevenção e detecção de ameaças, no controle de acessos e na rastreabilidade de eventos de segurança. A eficácia dessas soluções depende diretamente da manutenção do licenciamento ativo e da atualização contínua de suas funcionalidades, incluindo assinaturas de segurança, bases de dados, firmwares e módulos avançados de proteção. A interrupção desses serviços implicaria riscos significativos, como perda de mecanismos de detecção, obsolescência tecnológica, fragilização dos controles de acesso e comprometimento da capacidade de monitoramento e resposta a incidentes.

O levantamento das necessidades, foi realizado pela SAEB/SGI com base nos Planos de Contratações dos órgãos e entidades estaduais e evidenciou demanda recorrente e transversal pela continuidade dos serviços de licenciamento e atualização das soluções de segurança em uso, indispensáveis à sustentação operacional do ambiente corporativo de TIC. A ausência ou descontinuidade desses serviços impactaria diretamente a confiabilidade da infraestrutura tecnológica estadual e a prestação contínua de serviços digitais ao cidadão, contrariando princípios de eficiência e segurança da informação.

Além da renovação das licenças e atualizações, o escopo da contratação contempla a disponibilização de solução de segurança de rede destinada à segmentação lógica do tráfego interno, reforçando os controles entre ambientes, sistemas e perfis de acesso. Essa medida visa ampliar a proteção contra ameaças, assegurar a manutenção das funcionalidades ativas e garantir acesso às atualizações técnicas pertinentes, preservando a robustez e a confiabilidade do ambiente tecnológico estadual.

O Termo de Cooperação nº 054/2024, celebrado entre o Estado da Bahia, através da Secretaria da Administração do Estado da Bahia (Saeb) e a Companhia de Processamento de Dados do Estado da Bahia (Prodeb), autorizou a realização do procedimento licitatório, a ser realizado por meio do sistema de Registro de Preços em abril de 2024.

O referido procedimento licitatório teve como objeto a contratação de empresa especializada em Tecnologia da Informação e Comunicação, visando ao fornecimento de soluções de segurança, incluindo Next-Generation Firewalls (NGFW), soluções para endpoints, e-mail, autenticação de múltiplos fatores (MFA) e honeypot, possibilitando a adesão por órgãos e entidades da Administração Pública Estadual, tendo como resultado a entrega da solução do fabricante Fortinet pela empresa vencedora. Tal procedimento contemplou, ainda, a capacitação da equipe técnica local, garantindo a adequada operação das soluções adquiridas.

Seguem argumentos Técnicos e Estratégicos para mantermos a referida solução:

Compatibilidade e Integração

A permanência do mesmo fabricante garante compatibilidade total com a infraestrutura existente, evitando problemas de interoperabilidade entre diferentes tecnologias. Isso assegura a continuidade operacional sem necessidade de adaptações complexas ou substituições de componentes críticos.

Proteção do Investimento Realizado

A adoção de outro fabricante implicaria descarte parcial ou total dos ativos adquiridos, gerando desperdício de recursos públicos e aumento significativo de custos. A manutenção da solução atual preserva o investimento já realizado e otimiza o retorno esperado.

Redução de Custos Operacionais e de Treinamento

A equipe técnica já foi capacitada para operar a solução Fortinet, o que reduz custos adicionais com treinamentos e curva de aprendizado. A troca de fabricante demandaria novos treinamentos, impactando prazos e produtividade.

Mitigação de Riscos e Continuidade do Serviço

Alterações na arquitetura de segurança podem gerar vulnerabilidades temporárias e riscos à proteção dos dados. A permanência do fabricante atual assegura continuidade dos serviços críticos, evitando interrupções e garantindo conformidade com normas de segurança.

Escalabilidade e Atualizações

Diante do exposto, a manutenção do fabricante Fortinet revela-se a alternativa mais adequada para garantir a continuidade, a segurança e a eficiência das soluções já implantadas, preservando o investimento realizado, mitigando riscos operacionais e assegurando a conformidade com as diretrizes de governança e proteção da informação da Administração Pública do Estado da Bahia.

Em complementação, relacionamos abaixo os equipamentos de Soluções de Segurança Cibernética já existentes em Órgãos e Entidades da Administração Pública Estadual.

Marca	Produto	Descrição	PartNumber
Fortinet	FortiGate-3301E	Solução De Next Generation Firewall - NGFW	FG-3301E
Fortinet	Fortigate 600D	Solução De Next Generation Firewall– NGFW	FG-600D
Fortinet	Fortigate 600F	Solução De Next Generation Firewall– NGFW	FG-600F
Fortinet	Fortigate 3000D	Solução De Next Generation Firewall– NGFW	FG-3000D
Fortinet	Fortigate 3700F	Solução De Next Generation Firewall– NGFW	FG-3700F
Fortinet	FortiGate-200F	Solução De Next Generation Firewall - NGFW	FG-200F
Fortinet	FortiGate-100F	Solução De Next Generation Firewall - NGFW	FG-100F
Fortinet	FortiGate-80F	Solução De Next Generation Firewall - NGFW	FG-80F
Fortinet	Fortigate-60F	Solução De Next Generation Firewall– NGFW	FG-60F
Fortinet	Fortigate-61F	Solução De Next Generation Firewall– NGFW	FG-61F
Fortinet	Fortigate-40F	Solução De Next Generation Firewall– NGFW	FG-40F
Fortinet	Fortigate VM-08	Solução De Next Generation Firewall– NGFW	FG-VM08
Fortinet	FortiAnalyzer 3700F	Solução De Logs E Relatoria	FAZ-3700F
Fortinet	FortiAnalyzer 2000E	Solução De Logs E Relatoria	FAZ-2000E
Fortinet	FortiAnalyzer 300G	Solução De Logs E Relatoria	FAZ-300G
Fortinet	FortiAnalyzer 150G	Solução De Logs E Relatoria	FAZ-150G
Fortinet	FortiAuthenticator 3000E	Solução De Autenticação Centralizada	FAC-3000E
Fortinet	FortiManager 3000G	Solução De Gerência Centralizada	FMG-3000G
Fortinet	FortiManager 3900E	Solução De Gerência Centralizada	FMG-3000G
Fortinet	FortiWeb-2000F	Solução De Firewall De Aplicações WEB	FWB-2000F
Fortinet	FortiADC 400F	Solução Balanceamento De Carga De Aplicações	FAD-400F
Fortinet	FortiClient EMS EPP	Solução De Segurança De Endpoint E ZTNA	FortiClient EPP ZTNA
Fortinet	FortiMail 3000F	Solução De Segurança De Email	FortiMail 3000F
Fortinet	FortiSIEM	Solução De Correlação De Eventos, Resposta Automática E Remediação De Incidentes	FSM-AIO-BASE

3. JUSTIFICATIVA PARA UTILIZAÇÃO DO SISTEMA DE REGISTRO DE PREÇOS

Considerando as características do objeto, que envolve soluções de conectividade segura e de segurança da informação e cibersegurança, essenciais à continuidade dos serviços digitais e à operação das infraestruturas tecnológicas geridas pela PRODEB, constata-se a necessidade de contratações frequentes, enquadrando-se na hipótese prevista no inciso I do art. 122 do Regulamento de Licitações e Contratos (RLC) da PRODEB.

Ademais, as soluções a serem contratadas destinam-se ao atendimento de múltiplos órgãos e entidades da Administração Pública, usuários da infraestrutura de conectividade e segurança, conforme hipótese prevista no inciso III do art. 122 do RLC, favorecendo a padronização tecnológica, a governança centralizada e a racionalização dos esforços de contratação.

Soma-se a isso o fato de que, em razão da dinâmica de evolução tecnológica, expansão dos serviços e variação das demandas ao longo do tempo, não é possível definir previamente, com exatidão, os quantitativos a serem demandados durante toda a vigência contratual, atraindo também a aplicação do inciso IV do art. 122 do RLC.

Diante desse contexto, a adoção do Sistema de Registro de Preços mostra-se a alternativa mais adequada, por conferir maior flexibilidade administrativa, previsibilidade contratual e eficiência na gestão das contratações, em consonância com o disposto no art. 122 do RLC da PRODEB.

II. DO DETALHAMENTO DO OBJETO

4. DETALHAMENTO DO OBJETO

4.1. A especificação dos itens será detalhada nos Anexos integrantes deste TR.

4.2. LOTE 1 – REDE GOVERNO V

Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade estimada
1	02.81.00.00192352-8	Solução de Conectividade Segura TIPO 01 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 500MB.	Unidade	1.589
2	02.81.00.00192353-6	Solução de Conectividade Segura TIPO 02 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 2 links (redundância) de internet banda larga com velocidade de 500MB.	Unidade	707

3	02.81.00.00192354-4	Solução de Conectividade Segura TIPO 03 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 1GB.	Unidade	109
4	02.81.00.00192355-2	Solução de Conectividade Segura TIPO 04 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 2 links (redundância) de internet banda larga com velocidade de 1GB.	Unidade	167
5	02.81.00.00192356-0	Solução de Conectividade Segura TIPO 05 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários em unidades remotas que não possuem viabilidade de conexão via fibra ótica, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link satélite com velocidade de 100 MB.	Unidade	149
6	02.81.00.00192357-9	Solução de Conectividade Segura TIPO 06 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.	Unidade	101
7	02.81.00.00192358-7	Solução de Conectividade Segura TIPO 07 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SD-WAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 500MB.	Unidade	54

8	02.81.00.00192359-5	Solução de Conectividade Segura TIPO 08 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SD-WAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 500MB.	Unidade	16
9	02.81.00.00192360-9	Solução de Conectividade Segura TIPO 09 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SD-WAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 1GB.	Unidade	78
10	02.81.00.00192361-7	Solução de Conectividade Segura TIPO 10 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SD-WAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 1GB.	Unidade	33
11	02.81.00.00192362-5	Solução de Conectividade Segura TIPO 11 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SD-WAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB.	Unidade	91
12	02.81.00.00192363-3	Solução de Conectividade Segura TIPO 12 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SD-WAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB e 1 link de internet banda larga com velocidade de 500MB.	Unidade	14
13	02.81.00.00192364-1	Solução de Conectividade Segura TIPO 13 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades com até 40 usuários e que já possuem link de internet contemplando 01	Unidade	105

		firewall de próxima geração (NGFW) com tecnologia SD-WAN.		
14	02.81.00.00192365-0	Solução de Conectividade Segura TIPO 14 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades acima de 40 usuários e que já possuem link de internet contemplando 01 firewall de próxima geração (NGFW) com tecnologia SD-WAN.	Unidade	50
15	02.81.00.00192366-8	Solução de Conectividade Segura TIPO 15 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, 2 links (redundância) de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.	Unidade	20
16	02.81.00.00192367-6	Solução de Conectividade Segura TIPO 16 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, 2 links (redundância) de internet banda larga com velocidade de 1GB e 1 link satélite com velocidade de 100 MB.	Unidade	16
17	02.81.00.00192368-4	Solução de Conectividade Segura TIPO 17 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, destinada a unidades com até 05 usuários, contemplando 1 link de internet banda larga com velocidade de 200 Mbps e mecanismos de segurança providos de forma centralizada, sob gestão da PRODEB, sem a necessidade de firewall de borda dedicado na unidade.	Unidade	369
18	02.81.00.00192370-6	Serviço de Mudança de Endereço – até 300 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	137

19	02.81.00.00192371-4	Serviço de Mudança de Endereço – acima de 300 km até 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	144
20	02.81.00.00192372-2	Serviço de Mudança de Endereço – acima de 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	108
21	02.81.09.00008168-0	Solução de Operação e Monitoramento Central, prestada em regime contínuo e remunerada por valor mensal, dimensionada para atender até 500 (quinhentas) unidades de solução de conectividade segura em operação	Unidade	10
22	02.81.09.00008169-8	Solução de Monitoramento e Relatoria De Logs Tipo I	Unidade	02
23	02.81.00.00192944-5	Solução de Monitoramento e Relatoria De Logs Tipo II	Unidade	50
24	02.81.00.00192945-3	Solução de Monitoramento e Relatoria De Logs Tipo III	Unidade	04
25	02.81.00.00192946-1	UST – Unidade de Serviços Técnicos	Unidade	5.000

4.3. A utilização dos itens **da Solução de Conectividade Segura Tipos 07, 08, 09, 10, 11 e 12 (Lote 1)** ficará condicionada à aprovação prévia da SAEB e da PRODEB quanto à aderência e compatibilidade da solução de segurança alternativa a ser utilizada pelo órgão demandante. Nessas hipóteses, a gestão do equipamento de segurança deverá ser formalmente transferida para a PRODEB, assegurando a governança centralizada, a padronização operacional e a integração com os mecanismos corporativos de monitoramento e gestão da Rede Governo.

4.4. A utilização dos itens da **Solução de Conectividade Segura Tipos 13 e 14 (Lote 1)** será autorizada apenas de forma excepcional e transitória, restritos às hipóteses de necessidade de encerramento antecipado dos contratos vigentes de fornecimento da solução de segurança da Rede Governo IV, e somente até o término dos contratos atualmente vigentes de fornecimento de links da Rede Governo IV. Encerrado esse período transitório, tais soluções deverão ser obrigatoriamente substituídas por um dos itens das **Soluções Tipo 01, 02, 03, 04, 05 ou 06 (Lote 1)**, de modo a restabelecer o modelo pleno de conectividade segura integrada adotado para a Rede Governo V.

4.5. A utilização do item da **Solução de Conectividade Segura Tipos 17 (Lote 1)** ficará condicionada à aprovação prévia da SAEB e da PRODEB, mediante comprovação formal pelo órgão demandante de que a unidade se enquadra nos critérios técnicos estabelecidos para essa tipologia, bem como de que o serviço de gestão e monitoramento da Rede Governo encontra-se devidamente contratado junto à PRODEB. Tal condicionante decorre do fato de que, nessa modalidade, os mecanismos de segurança da informação são providos de forma centralizada pela PRODEB, sendo imprescindível assegurar a integração plena com a governança, o monitoramento corporativo e as políticas de segurança da Rede Governo.

4.6. O conjunto desses itens (Lote 1) constitui, de forma integrada, a solução corporativa de conectividade segura da Rede Governo, permitindo atender, de maneira padronizada, escalável e governada, a diversidade de

unidades administrativas, perfis de uso e níveis de criticidade existentes no âmbito do Poder Executivo Estadual.

4.7. Os itens 21 a 25 serão consumidos exclusivamente pela Prodeb, por serem necessários à viabilização do monitoramento técnico e operacional da Rede Governo, bem como ao suporte às atividades de gestão, operação e evolução da infraestrutura sob sua responsabilidade.

4.8. LOTE 2 – SOLUÇÕES DE SEGURANÇA

Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade estimada
1	02.81.00.00192373-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600E, pelo período de 12 meses	Unidade	04
2	02.81.00.00192374-9	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 601IE, pelo período de 12 meses	Unidade	04
3	02.81.00.00192375-7	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 400F, pelo período de 12 meses	Unidade	08
4	02.81.00.00192376-5	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200F, pelo período de 12 meses	Unidade	09
5	02.81.00.00192377-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200E, pelo período de 12 meses	Unidade	04
6	02.81.00.00192378-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 100F, pelo período de 12 meses	Unidade	24
7	02.81.00.00192379-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 80F, pelo período de 12 meses	Unidade	12
8	02.81.00.00192380-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 60F, pelo período de 12 meses	Unidade	300
9	02.81.00.00192381-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 61F, pelo período de 12 meses	Unidade	300
10	02.81.00.00192382-0	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 150G, pelo período de 12 meses	Unidade	04

11	02.81.00.00192383-8	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 300G, pelo período de 12 meses	Unidade	04
12	02.81.00.00192384-6	Serviço de Licenciamento e Atualização das Funcionalidades de Autenticação Centralizada de Usuários Marca Fortinet Modelo FortiAuthenticator 800F, pelo período de 12 meses	Unidade	04
13	02.81.00.00192385-4	Solução De Segurança de Rede NGFW TIPO I, com licenciamento pelo período de 12 meses	Unidade	04
14	02.81.00.00192386-2	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede - Segmentação Interna TIPO I, pelo período de 12 meses	Unidade	04
15	02.81.00.00192947-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3700F, pelo período de 12 meses	Unidade	04
16	02.81.00.00192948-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3301E, pelo período de 12 meses	Unidade	04
17	02.81.00.00192949-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3000D, pelo período de 12 meses	Unidade	02
18	02.81.00.00192950-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600F, pelo período de 12 meses	Unidade	04
19	02.81.00.00192951-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 40F, pelo período de 12	Unidade	60
20	02.81.00.00192952-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate-VM08, pelo período de 12 meses	Unidade	02
21	02.81.00.00192953-4	Serviço de Licenciamento e Atualização das Funcionalidades de WAF Marca Fortinet Modelo FortiWeb-2000F, pelo período de 12 meses	Unidade	04
22	02.81.00.00192954-2	Serviço de Licenciamento e Atualização das Funcionalidades de ADC Marca Fortinet Modelo FortiADC-400F, pelo período de 12 meses	Unidade	02
23	02.80.00.00192955-0	Serviço de Licenciamento e Atualização das Funcionalidades de Gerenciador Centralizada de Dispositivos Marca Fortinet Modelo FortiManager 3000G, pelo período de 12 meses	Unidade	02
24	02.81.00.00192956-9	Serviço de Licenciamento e Atualização das Funcionalidades de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	02

25	02.81.00.00192957-7	Serviço de Upgrade para 50 Devices e 500 EPS de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	04
26	02.81.00.00192958-5	Solução De Segurança de Aplicações WAF - TIPO I, com licenciamento pelo período de 12 meses	Unidade	02
27	02.81.00.00192959-3	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF - TIPO I, pelo período de 12 meses	Unidade	02
28	02.81.00.00192989-5	Solução De Segurança de Aplicações WAF - TIPO II, com licenciamento pelo período de 12 meses	Unidade	10
29	02.81.00.00192990-9	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF - TIPO II, pelo período de 12 meses	Unidade	10
30	02.81.00.00192962-3	Solução De Segurança de Aplicações WAF para Ambientes Híbridos, com licenciamento pelo período de 12 meses	Unidade	10
31	02.81.00.00192963-1	Serviço de Licenciamento e Atualização das Funcionalidades de Solução De Segurança de Aplicações WAF para Ambientes Híbridos, pelo período de 12 meses	Unidade	10
32	02.81.00.00192964-0	Solução de Segurança Decoy/Honeypot, com licenciamento pelo período de 12 meses	Unidade	06
33	02.81.00.00192965-8	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança Decoy/Honeypot, pelo período de 12 meses	Unidade	06
34	02.81.00.00192966-6	Solução De Segurança de Rede NGFW TIPO II, com licenciamento pelo período de 12 meses	Unidade	100
35	02.81.00.00192967-4	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede - Segmentação Interna TIPO II, pelo período de 12 meses	Unidade	100
36	02.81.00.00192968-2	Solução De Segurança de Rede NGFW TIPO III, com licenciamento pelo período de 12 meses	Unidade	50
37	02.81.00.00192969-0	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede - Segmentação Interna TIPO III, pelo período de 12 meses	Unidade	50

4.8.1. A contratada deverá proporcionar treinamento “hands on” aos colaboradores da contratante, abrangendo a operação, manutenção, geração de relatórios e uso das funcionalidades da solução.

5. DETALHAMENTO DO SERVIÇO

5.1. O **recebimento provisório** consiste no ato formal pelo qual a Contratante atesta a entrega inicial do objeto contratado, permitindo a conferência de sua conformidade. Nessa etapa, registra-se que o bem ou serviço foi disponibilizado pelo contratado, ficando sujeito à verificação detalhada, testes e eventuais ajustes. Somente após essa análise é efetuado o recebimento definitivo, que confirma o atendimento integral às exigências do contrato e do Termo de Referência.

5.2. O **recebimento definitivo** é o ato formal pelo qual a Contratante, após a verificação detalhada do objeto entregue, atesta que o bem ou serviço atende integralmente às especificações do contrato e do Termo de

Referência. Nessa etapa, confirma-se a conformidade, o funcionamento e a adequação do objeto, bem como o cumprimento de todas as obrigações pelo contratado, formalizando a aceitação final da contratação.

5.3. O termo de homologação consiste na confirmação final de que o serviço contratado foi executado de forma satisfatória e em conformidade com as especificações estabelecidas no contrato e no Termo de Referência. A homologação ocorre, quando aplicável, após a verificação da execução completa do serviço, como treinamentos, instalações, parametrizações, configurações ou outras atividades, certificando que todos os requisitos foram atendidos e que não há pendências técnicas ou operacionais.

LOTE 1

5.4. Modalidades de execução do serviço – Lote 1

A execução do serviço de conectividade segura observará modelo estruturado de trabalho, baseado na delegação clara de responsabilidades entre a Administração e a contratada, cabendo à Administração a definição das demandas e o acompanhamento qualitativo dos resultados, e à contratada a responsabilidade integral pela execução operacional dos serviços, compreendendo planejamento, implantação, operação, monitoramento, suporte e gestão continuada da solução contratada.

A execução deverá contemplar, de forma integrada e coordenada, as etapas de elaboração de projeto executivo, implantação da solução de conectividade segura, implantação e integração dos mecanismos de monitoramento, operação assistida, monitoramento contínuo, suporte técnico e capacitação, assegurando a plena operacionalização da solução e a continuidade dos serviços ao longo da vigência contratual. Nenhuma etapa de execução poderá ser iniciada sem a prévia aprovação formal da Administração, devendo a contratada observar rigorosamente as diretrizes estabelecidas nos instrumentos do certame.

O modelo de execução deverá considerar a abrangência territorial da Rede Governo, com atendimento às unidades administrativas distribuídas em todo o Estado da Bahia, respeitada a classificação por macrorregiões e a necessidade de atendimento remoto ou presencial, conforme a natureza das atividades e a criticidade dos serviços. A solução deverá operar em regime de disponibilidade contínua, com mecanismos de monitoramento e resposta a incidentes compatíveis com a criticidade dos serviços prestados à Administração Pública Estadual.

As modalidades específicas de execução, os fluxos operacionais, os procedimentos de acompanhamento, os níveis de serviço, os critérios de aceitação e os mecanismos de controle e sanção serão detalhados neste documento, no edital e nos instrumentos contratuais, em consonância com as diretrizes estabelecidas no Estudo Técnico Preliminar.

5.5. Serviços a serem executados pela CONTRATADA - Lote 1

- 5.5.1. Projeto Executivo: Elaboração de projeto técnico detalhado para implantação da solução, conforme parâmetros deste Termo de Referência, topologia de rede, cronograma e lista de equipamentos.
- 5.5.2. Implantação das Soluções de Conectividade Segura: Instalação e configuração de todos os equipamentos, softwares e integrações necessárias para operação plena da solução, incluindo testes de aceitação.
- 5.5.3. Implantação do Centro de Monitoramento Integrado: Instalação e configuração conforme especificações, contemplando ajustes finos e integração com sistemas existentes.
- 5.5.4. Monitoramento: Implementação de processos e ferramentas para acompanhamento dos equipamentos do Centro de Monitoramento Integrado e das Soluções de Conectividade Segura, incluindo disponibilidade dos links de internet e rede local, em tempo real, com indicadores de desempenho e alarmes para resposta rápida a incidentes.
- 5.5.5. Suporte Técnico: Atendimento de incidentes e resolução de problemas técnicos relacionados à solução fornecida, de forma remota ou presencial, conforme criticidade e SLAs estabelecidos.
- 5.5.6. Treinamento: Capacitação referente ao Lote 1, item 21 - Solução de Gestão, Operação e Monitoramento Central, abrangendo operação, manutenção, geração de relatórios e uso das funcionalidades da solução, conforme detalhamento no Anexo de Especificações Técnicas da Rede Governo.

5.6. Serviços Implantação das Soluções - Lote 1

5.6.1. Após a assinatura do contrato, deverá ser realizada uma reunião de alinhamento entre a CONTRATANTE e CONTRATADA, para detalhamento das etapas de instalação, configuração, migração e demais itens referentes aos serviços contratados, seguindo o cronograma e as etapas descritas na tabela abaixo:

CRONOGRAMA DE IMPLANTAÇÃO DAS SOLUÇÕES				
ID	Evento	Quando	Prazo em dias até	Quem
1	Assinatura do Contrato e publicação	Início	Não se aplica	Ambos
2	Reunião de Alinhamento	Após ID 1	5 dias úteis	Ambos
3	Entrega do Projeto Executivo	Após ID 1	10 dias úteis	Contratada
4	Implantação do Centro de Monitoramento	Após ID 1	20 dias úteis	Contratada
5	Formalização da Solicitação de Implantação	Início	Não se aplica	Ambos
6	Início Atividade de Implantação conforme Macrorregião	Após ID 5	Imediatamente	Contratada
7	Implantação Macrorregião 01-Salvador e localidade até 50 km	Após ID 6	25 dias úteis	Contratada
8	Implantação Macrorregião 02-Entre 50 e 300 km de Salvador	Após ID 6	30 dias úteis	Contratada
9	Implantação Macrorregião 03- Acima de 300 km de Salvador	Após ID 6	35 dias úteis	Contratada
10	Documento de implantação para a homologação da instalação dos equipamentos	Após ID 7, 8, 9	3 dias úteis	Contratada
11	Recebimento Definitivo relativo entregue, instalado e operando.	Após ID 10	3 dias úteis	Contratante
12	Início dos Serviços	Após ID 7, 8, 9	Imediatamente	Contratada
13	Entrega do Relatório de Operação Mensal	Mensal após início	5º dia útil do mês	Contratada
14	Aferição do Nível Mínimo de Serviço	Após ID 13	2 dias úteis	Contratante
15	Pagamento dos serviços	Após ID 14	8 dias úteis	Contratante

- 5.6.2. Durante a instalação, os profissionais da CONTRATADA deverão informar todas as ações executadas para os profissionais indicados pela CONTRATANTE;
- 5.6.3. Entende-se por instalação dos equipamentos: a montagem física e acessórios fornecidos, bem como a configuração lógica de todos os equipamentos e softwares envolvidos;
- 5.6.4. Entende-se por instalação dos softwares a disponibilização em pleno funcionamento, configurado e licenciado pelo prazo especificado no respectivo item do Termo de Referência;
- 5.6.5. Após a assinatura do instrumento contratual e até a entrega dos equipamentos, serão realizadas reuniões preparatórias, remotas ou presenciais, caso necessários, com a presença dos integrantes da equipe técnica da CONTRATADA, da qual se lavrará ata para permitir o acompanhamento criterioso da execução do objeto;
- 5.6.6. Será apresentado o ambiente atual da CONTRATANTE, onde a CONTRATADA deverá levantar todos os requisitos e configurações pertinentes à referida implantação;
- 5.6.7. Será apresentado pela CONTRATADA o Plano de Instalação, contemplando o que será migrado, as funcionalidades que serão implementadas segundo o Termo de Referência;
- 5.6.8. O Plano de Instalação poderá ser recusado pela CONTRATANTE, devendo a CONTRATADA realizar os ajustes definidos em reunião e reapresentá-los;

- 5.6.9. A CONTRATADA, depois de concluído o serviço de instalação, deverá realizar, com acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para validar a referida instalação de acordo com o respectivo Plano;
- 5.6.10. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter nome, data e assinatura do técnico responsável da CONTRATADA;
- 5.6.11. A documentação deverá ser entregue em meio digital (formatos PDF e DOCx);
- 5.6.12. A documentação deverá ser validada pela equipe técnica da CONTRATANTE, devendo ser ajustada pela CONTRATADA caso seja solicitado.
- 5.6.13. Todos os serviços dos itens devem ocorrer de maneira remota ou local, quando necessário, no Estado da Bahia.
- 5.6.14. Após a aprovação da documentação pela CONTRATANTE, caracterizando a conclusão dos serviços de instalação, configuração e operação assistida, a CONTRATANTE emitirá o Termo de Homologação, no prazo de até 3 (três) dias úteis, contado da entrega/recebimento da documentação prevista no cronograma do item 5.6.;
- 5.6.15. Durante a etapa de homologação, caso a equipe técnica da CONTRATANTE identifique inconformidade na implantação da solução instalada, é de responsabilidade da CONTRATADA, iniciar as devidas correções num prazo de 3 (três) dias úteis após a emissão do relatório de inconformidade;
- 5.6.16. Não haverá custos adicionais à CONTRATANTE para a realização das correções apontadas, sendo necessária a atualização da documentação, que foi entregue na etapa de instalação para que a CONTRATANTE realize nova homologação da solução, iniciando-se um novo prazo a ser acordado entre as partes para resolução definitiva das inconformidades identificadas;
- 5.6.17. Quando aplicável, na hipótese prevista no item 2.1.1 (Base Implantada), os equipamentos substitutos e demais componentes necessários à compatibilidade com a infraestrutura existente deverão ser entregues e devidamente instalados no Data Center da PRODEB no prazo máximo de até 60 (sessenta) dias corridos, contado da assinatura do contrato, às expensas da CONTRATADA.

LOTE 2

5.7. Modalidades de execução do serviço - Lote 2

- 5.7.1. A execução dos serviços decorrentes da Ata de Registro de Preços ocorrerá de forma descentralizada, mediante a formalização de contratações específicas pelos órgãos e entidades do Poder Executivo Estadual, conforme suas necessidades e disponibilidades orçamentárias, observadas as condições, os limites e os parâmetros estabelecidos neste Termo de Referência.
 - 5.7.2. Os serviços serão executados em regime continuado, abrangendo o licenciamento ativo e a atualização das funcionalidades das soluções de segurança da informação, bem como, quando aplicável, a disponibilização da solução de segurança de rede destinada à segmentação lógica do tráfego interno, nos prazos e condições definidos nos instrumentos contratuais derivados da ata.
 - 5.7.3. A execução deverá ocorrer em conformidade com as especificações técnicas, com os níveis de serviço e com as condições contratuais definidos, de modo a garantir a continuidade, a regularidade e a confiabilidade dos serviços de segurança da informação que suportam o ambiente corporativo de TIC do Estado.
- 5.8.** Os equipamentos serão recebidos provisoriamente, no prazo de 05 (cinco) dias contados da entrega, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta comercial;
- 5.9.** O(s) equipamento(s) deve(m) ser novo(s), sem prévia utilização, não remanufaturados, de primeiro uso e acondicionados adequadamente em caixa lacrada de fábrica, conforme recomendações do fabricante, de forma a propiciar completa segurança durante o transporte;
- 5.10.** Os equipamentos poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 30 (trinta) dias, a contar da notificação a CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades;

- 5.11. Os equipamentos serão recebidos definitivamente no prazo de 5 (cinco) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material, e consequente aceitação, mediante termo de recebimento definitivo;
- 5.12. O recebimento definitivo dos bens está condicionado à conclusão do serviço de instalação dos mesmos.
- 5.13. A CONTRATADA deverá entregar toda documentação comprobatória do licenciamento de softwares e da garantia.

6. ACORDO DE NÍVEL DE SERVIÇOS

LOTE 1

6.1. Níveis de Serviço de Atendimento para Incidentes – Lote 1

6.1.1. A CONTRATADA deverá garantir o cumprimento dos seguintes prazos de atendimento técnico, classificados por criticidade, localização geográfica e modalidade (local ou remoto), assegurando a continuidade operacional do Centro de Monitoramento Integrado e das demais unidades do CONTRATANTE, conforme tabela abaixo:

Tipo de Unidade	Nível de Severidade	Atendimento	Prazo (SLA)
Centro de Monitoramento Integrado	Severidade Crítica	Local	04 horas corridas
	Severidade Alta	Local	06 horas corridas
	Severidade Média	Local e ou remoto	08 horas úteis
	Solicitação Serviço	Local e ou remoto	10 horas úteis
Solução de Conectividade do Tipo 01 a 17	Severidade Crítica	Local	04 horas corridas
	Severidade Alta	Local	10 horas corridas
	Severidade Média	Local e ou Remoto	06 horas úteis
	Solicitação Serviço	Local e ou Remoto	08 horas úteis

6.1.2. Classificação dos Níveis de Severidade

6.1.2.1. **Severidade Crítica** - Solução de segurança inoperante, sem alternativa de contorno, causando indisponibilidade em sistemas/serviços produtivos que dependem desse ativo.

6.1.2.2. **Severidade Alta** - Problema na solução que impacta em determinado sistema/serviço produtivos que dependem desse ativo. Falha parcial que não impedem o funcionamento da solução, porém afeta determinados sistemas.

6.1.2.3. **Severidade Média** - Problema contornável que não gera qualquer impacto aos sistemas/serviços produtivos que dependem desses ativos.

6.1.3. Observações complementares

6.1.3.1. Incluem-se unidades periféricas conectadas diretamente à infraestrutura central.

6.1.3.2. Os prazos consideram deslocamento por via terrestre em condições normais de tráfego.

6.1.3.3. Pode incluir necessidade de pernoite de equipe técnica no local de atendimento.

6.1.4. O prazo de atendimento técnico compreende desde o registro formal da ocorrência, feito pelo contratante, até o restabelecimento dos serviços afetados, assegurando a continuidade operacional com todo escopo do serviço em pleno funcionamento

6.1.5. A indisponibilidade total será caracterizada quando o serviço estiver 100% inoperante, impossibilitando o cumprimento das atividades essenciais.

6.1.6. Não serão consideradas indisponibilidades as seguintes situações:

6.1.6.1. Janela de manutenção previamente acordada entre CONTRATANTE e CONTRATADA;

- 6.1.6.2. Indisponibilidade da CONTRATANTE em realizar tarefas que dependam desta;
- 6.1.6.3. Paradas programadas pela CONTRATADA e aprovadas pelo CONTRATANTE. Neste caso, a autorização deve ser solicitada pela CONTRATADA com, pelo menos, 5 (cinco) dias de antecedência;
- 6.1.6.4. Paradas ocasionadas nos equipamentos por erros de configuração causados pelo CONTRATANTE, sem responsabilidade da CONTRATADA;

6.2. Níveis de Serviço de Atendimento para Solicitações de Suporte – Lote 1

6.2.1. A CONTRATADA deverá garantir o cumprimento dos seguintes prazos de atendimento técnico, para solicitações de serviços, assegurando a continuidade operacional conforme tipos de solicitação:

6.2.1.1. Serviços de Suporte ajuste de configurações de link e equipamentos:

6.2.1.1.1. Atendimento Técnico Remoto – Demais Unidades do CONTRATANTE

6.2.1.1.2. Prazo máximo: até 04 (quatro) horas úteis.

6.2.1.2. Tipos de Solicitação de Serviço e Suporte:

6.2.1.2.1. Análises Técnicas

6.2.1.2.1.1. Diagnóstico de indisponibilidade parcial ou total do equipamento NGFW;

6.2.1.2.1.2. Verificação de consumo de CPU, memória e sessões simultâneas;

6.2.1.2.1.3. Análise de logs de tráfego, eventos de segurança e relatórios do NGFW;

6.2.1.2.1.4. Identificação de gargalos de desempenho ou latência;

6.2.1.2.1.5. Análise de eventos críticos gerados por IPS, AntiVirus, Web Filtering, Application Control, SSL Inspection, entre outros módulos;

6.2.1.2.1.6. Auditoria de políticas e regras de firewall para identificar sobreposições ou conflitos;

6.2.1.2.1.7. Verificação e recomendação de otimização em tabelas de roteamento e políticas de SD-WAN.

6.2.1.2.2. Alterações de Parâmetros

6.2.1.2.2.1. Inclusão, modificação ou exclusão de regras de firewall (políticas com ou sem NAT);

6.2.1.2.2.2. Ajuste de perfis de segurança (Web Filter, Application Control, IPS, etc.);

6.2.1.2.2.3. Alterações em objetos de rede (endereços, grupos, serviços, FQDNs);

6.2.1.2.2.4. Atualização de listas de bloqueio/permitidos (whitelist/blacklist) para IPs, URLs e aplicações;

6.2.1.2.2.5. Alteração de parâmetros de VPN (IPsec VPN), incluindo criação ou ajuste de túneis;

6.2.1.2.2.6. Configuração de alta disponibilidade (HA) ou balanceamento de carga;

6.2.1.2.2.7. Ajuste de thresholds para alertas de segurança e performance.

6.2.1.2.2.8. Consultas Operacionais

6.2.1.2.2.9. Apoio na interpretação de logs e relatórios gerados pelo NGFW;

6.2.1.2.2.10. Orientação sobre a priorização de tráfego (QoS, Traffic Shaping);

6.2.1.2.2.11. Esclarecimento de funcionamento de módulos de segurança;

6.2.1.2.2.12. Apoio em decisões para atualização de firmware e aplicação de patches;

- 6.2.1.2.2.13. Recomendação de boas práticas de configuração e hardening;
- 6.2.1.2.2.14. Esclarecimento sobre funcionamento de políticas UTM e NGFW;
- 6.2.1.2.2.15. Apoio na integração do NGFW com sistemas de autenticação (LDAP, RADIUS, SAML, etc.).
- 6.2.1.2.3. Suporte Geral
 - 6.2.1.2.3.1. Correção de falhas de configuração;
 - 6.2.1.2.3.2. Aplicação de atualizações de segurança e correção de vulnerabilidades;
 - 6.2.1.2.3.3. Testes de failover e redundância;
 - 6.2.1.2.3.4. Backup e restauração de configurações;
 - 6.2.1.2.3.5. Configuração e manutenção de logs para integração com ferramentas;
 - 6.2.1.2.3.6. Apoio na configuração de alertas e monitoramento proativo;
 - 6.2.1.2.3.7. Orientação em situações de incidente de segurança detectadas pelo NGFW;
 - 6.2.1.2.3.8. Reconfiguração ou substituição de equipamento em caso de falha física.

LOTE 2

6.3. Níveis de Serviço de Atendimento para Solicitações – Lote 2

6.3.1. A CONTRATADA deverá garantir o cumprimento dos seguintes prazos de atendimento técnico, para solicitações de serviços, assegurando a continuidade operacional conforme tipos de solicitação:

Tipo de Solicitação	SLA de Resposta (Início)	SLA de Solução (ou Contorno)
Requisição de Serviço PRODEB	Até 02 horas úteis	Até 16 horas úteis
Requisição de Serviço demais unidades	Até 06 horas úteis	Até 18 horas úteis

6.3.1.1. Tipos de Solicitação de Serviço:

- 6.3.1.1.1. Diagnóstico de Anomalias: Análise remota imediata em casos de indisponibilidade parcial ou total dos equipamentos (NGFW/WAF).
- 6.3.1.1.2. Tratamento de Incidentes de Segurança: Mitigação ativa de ataques detectados (DDoS L7, tentativas de intrusão) através da aplicação de contra-medidas nas configurações.
- 6.3.1.1.3. Correção de Falhas de Conectividade: Restabelecimento de túneis VPN (IPsec/SSL) e ajustes de rotas em caso de quedas de links.
- 6.3.1.1.4. Depuração de Tráfego: Análise profunda de pacotes (packet sniffing) para identificar a causa raiz de latências ou perdas de pacotes.
- 6.3.1.1.5. Ajustes Paramétricos de WAF: Refinamento contínuo (fine-tuning) de assinaturas e regras de proteção web para eliminação de falsos positivos e adequação a novas aplicações publicadas.
- 6.3.1.1.6. Gestão de Regras de Controle de Acesso: Criação, modificação e revogação de regras de firewall, NAT e políticas de roteamento SD-WAN conforme a necessidade da CONTRATANTE.
- 6.3.1.1.7. Segmentação Lógica: Configuração de VLANs e zonas de segurança para isolamento de redes críticas.

- 6.3.1.1.8. Atualização de Ativos (Patch Management): Aplicação remota de atualizações de firmware e correções de segurança (patches) recomendadas pelo fabricante para manter a integridade do ambiente.
- 6.3.1.1.9. Auditoria de Configuração: Revisão periódica das políticas de segurança para identificar regras obsoletas, duplicadas ou inseguras (shadow rules).
- 6.3.1.1.10. Análise de Capacidade (Capacity Planning): Monitoramento de consumo de recursos (CPU, Memória, Sessões) com alertas para evitar saturação.
- 6.3.1.1.11. Verificação de Alta Disponibilidade (HA): Testes assistidos de failover para assegurar que o equipamento secundário assumirá a carga em caso de falha do primário.
- 6.3.1.1.12. Gestão de Backups: Execução e validação de cópias de segurança das configurações dos equipamentos.
- 6.3.1.1.13. Atualização de Firmware e Patches: Planejamento e execução remota de atualizações de sistema operacional (OS) para correção de vulnerabilidades (CVEs) e bugs, com validação de backup prévio.
- 6.3.1.1.14. Gestão de Assinaturas de Segurança: Verificação diária da atualização das bases de dados de ameaças (IPS, AV, Botnet, URL filtering).
- 6.3.1.1.15. Monitoramento de Recursos: Análise contínua de consumo de CPU, Memória, Disco, Sessões Simultâneas e temperatura (via SNMP/API).
- 6.3.1.1.16. Backup de Configurações: Rotina automatizada de backup diário das configurações e verificação de integridade dos arquivos.
- 6.3.1.1.17. Teste de Failover (HA): Apoio remoto na realização de testes periódicos de Alta Disponibilidade (Cluster Ativo-Ativo ou Ativo-Passivo) para validar a redundância.
- 6.3.1.1.18. Troubleshooting Avançado: Diagnóstico de falhas de conectividade, perda de pacotes, latência e indisponibilidade de aplicações.
- 6.3.1.1.19. Análise de Logs e Auditoria: Interpretação de logs de tráfego (Traffic Logs) e de eventos (Event Logs) para identificar a causa raiz de incidentes.
- 6.3.1.1.20. Resposta a Ameaças: Atuação imediata para bloqueio de IPs de origem maliciosa, isolamento de hosts comprometidos e mitigação de ataques em andamento detectados pelo IPS/WAF.

7. DESCONTOS POR DESCUMPRIMENTO DOS NÍVEIS DE SERVIÇO

LOTE 1

7.1. Procedimentos para descontos no pagamento – Lote 1

7.1.1. Base de Cálculo

- 7.1.1.1. O desconto será calculado sobre o valor mensal da solução afetada.

7.1.2. Período de Apuração

- 7.1.2.1. A apuração dos níveis de serviço observará a base temporal definida para cada indicador de desempenho, conforme estabelecido nos Acordos de Nível de Serviço (ANS).
- 7.1.2.2. Para indicadores definidos em regime de **horas úteis**, considera-se o horário de 08h00 às 18h00, de segunda a sexta-feira, exceto feriados.
- 7.1.2.3. Para indicadores definidos em regime de **horas corridas (24x7)**, a apuração deverá considerar integralmente o tempo decorrido, incluindo períodos noturnos, finais de semana e feriados.

7.1.2.4. O monitoramento da disponibilidade dos serviços será realizado por meio da solução de monitoramento contratada, a qual deverá ser devidamente homologada pela CONTRATANTE e configurada e mantida pela CONTRATADA, constituindo-se como a fonte oficial e exclusiva de registro da disponibilidade para fins de acompanhamento, apuração de níveis de serviço e aplicação das disposições contratuais pertinentes.

7.1.3. Medição da Disponibilidade

7.1.3.1. A disponibilidade será medida automaticamente por sistema de monitoramento disponibilizado pela CONTRATADA, contemplando todos os dias do mês.

7.1.3.2. A apuração do Nível Mínimo de Serviço (NMS) observará a base temporal definida no respectivo indicador, podendo considerar horas úteis ou horas corridas, conforme especificado nos ANS.

7.1.3.3. Será admitida tolerância de até 5% do período de apuração definido para o indicador no mês vigente.

7.1.3.4. A disponibilidade exigida será calculada considerando o total de horas do período de apuração definido para o respectivo indicador de nível de serviço, admitindo-se tolerância de até 5% (cinco por cento) de indisponibilidade no período.

A apuração obedecerá à seguinte fórmula:

$$\text{Disponibilidade (\%)} = (\text{Tempo Total} - \text{Tempo Indisponível}) / \text{Tempo Total} \times 100$$

Onde:

- **Tempo Total:** corresponde ao total de horas do período de apuração do indicador, podendo ser definido em horas úteis ou horas corridas, conforme o ANS;
- **Tempo Indisponível:** corresponde ao somatório dos períodos de indisponibilidade registrados no período de apuração.

Exemplo 1 – Horas úteis: 220 horas → tolerância 11h → disponibilidade mínima 95%

Exemplo 2 – 24x7: 720 horas → tolerância 36h → disponibilidade mínima 95%

7.1.4. Desconto por Descumprimento dos Prazos de Atendimento

7.1.4.1. Na hipótese de não atendimento aos níveis de serviço especificados, sem prejuízo das sanções administrativas previstas no contrato e na legislação vigente, serão aplicados os descontos previstos na tabela abaixo, os quais serão descontados da garantia prestada pela CONTRATADA, em razão do descumprimento da qualidade mínima exigida.

Tipo de Atraso	Metodologia de Descontos
Resolução de chamados de solicitação de serviço	Desconto de 0,005% do valor da fatura mensal
Resolução de chamados de suporte técnico com severidade Média	Desconto de 0,5% do valor da parcela mensal da solução afetada
Resolução de chamados de suporte técnico com severidade Alta	Desconto de 1,0% do valor da parcela mensal da solução afetada
Resolução de chamados de suporte técnico com severidade Crítica	Desconto de 2,0% do valor da parcela mensal da solução afetada

7.1.4.2. Para fins de aplicação de descontos, os indicadores de nível de serviço observarão as seguintes diretrizes:

- Considera-se solução afetada aquela diretamente impactada pela ocorrência registrada, podendo corresponder, conforme o caso, à solução de conectividade, à solução de segurança, à solução de monitoramento central, à solução de relatórios ou a outro componente da solução contratada diretamente relacionado à ocorrência.

II – As solicitações de serviço referem-se aos serviços descritos nos itens 6.2.1.2 e 6.3.1.1 deste Termo de Referência.

- 7.1.4.3. Os descontos previstos na tabela acima serão calculados com base no valor mensal da solução afetada e poderão, a critério da CONTRATANTE, ser descontados dos valores devidos à CONTRATADA na fatura do período ou da garantia contratual.
- 7.1.4.4. O valor do desconto no período será igual ao somatório das ocorrências de não atendimento ou solução nos níveis de serviço especificados.
- 7.1.4.5. Os descontos aplicados só poderão ser relevados motivadamente e por conveniência administrativa, mediante ato da autoridade competente, devidamente justificado.
- 7.1.4.6. Caso o desconto a ser aplicado seja superior ao valor da garantia, além da perda desta, responderá o contratado pela sua diferença, ou quando for o caso, cobrada judicialmente.
- 7.1.4.7. A garantia deverá ser restabelecida integralmente, caso tenha incidido qualquer desconto sobre o valor desta.

LOTE 02

7.2. Desconto por Descumprimento dos Prazos de Atendimento

- 7.2.1. Na hipótese de não atendimento aos níveis de serviço especificados, sem prejuízo das sanções administrativas previstas no contrato e na legislação vigente, serão aplicados os descontos previstos na tabela abaixo, os quais serão descontados da garantia prestada pela CONTRATADA, em razão do descumprimento da qualidade mínima exigida.

Tipo de Atraso	Metodologia de Descontos
Resolução de chamados dos serviços de garantia com severidade Média	Desconto de 0,01% do valor do item por hora útil que exceder os níveis de acordo, a ser descontado do valor da garantia
Resolução de chamados dos serviços de garantia com severidade Alta	Desconto de 0,02% do valor do item por hora útil que exceder os níveis de acordo, a ser descontado do valor da garantia
Resolução de chamados dos serviços de garantia com severidade Crítica	Desconto de 0,03% do valor do item por hora útil que exceder os níveis de acordo, a ser descontado do valor da garantia

- 7.2.2. Os descontos previstos na tabela acima serão calculados com base no valor do item e serão descontados da garantia prestada pela empresa contratada.
- 7.2.3. O valor do desconto no período será igual ao somatório das ocorrências de não atendimento ou solução nos níveis de serviço especificados.
- 7.2.4. Os descontos aplicados só poderão ser relevados motivadamente e por conveniência administrativa, mediante ato da autoridade competente, devidamente justificado.
- 7.2.5. Caso o desconto a ser aplicado seja superior ao valor da garantia, além da perda desta, responderá o contratado pela sua diferença, ou quando for o caso, cobrada judicialmente.
- 7.2.6. A garantia deverá ser restabelecida integralmente, caso tenha incidido qualquer desconto sobre o valor desta.

8. SUPORTE TÉCNICO E MANUTENÇÃO

LOTE 01

- 8.1.** A solução de conectividade segura deverá ser concebida, implantada e operada de modo a assegurar manutenção contínua, suporte técnico permanente e sustentação operacional compatível com ambientes governamentais de missão crítica, considerando a elevada dependência dos serviços públicos estaduais em relação à disponibilidade, ao desempenho e à segurança da Rede Governo.
- 8.2.** A manutenção da solução deverá abranger, de forma integrada e indivisível, todos os seus componentes de conectividade, segurança, monitoramento e gestão, contemplando atividades de manutenção preventiva, corretiva, adaptativa e evolutiva. A solução deverá permitir a realização dessas atividades de forma controlada e planejada, com mitigação de riscos operacionais e preservação da continuidade dos serviços essenciais, admitindo janelas de manutenção previamente acordadas e devidamente comunicadas.
- 8.3.** O suporte técnico deverá ser prestado de forma contínua e ininterrupta, compatível com a criticidade da infraestrutura suportada e com a abrangência territorial da Rede Governo. A solução deverá ser capaz de suportar atendimento remoto e presencial, conforme a natureza da ocorrência, o impacto operacional identificado e a localização das unidades atendidas, assegurando a pronta atuação sobre falhas, incidentes de segurança, degradações de desempenho e demais eventos que possam comprometer a operação da rede.
- 8.4.** A solução deverá prever mecanismos estruturados de registro, classificação, acompanhamento e tratamento de incidentes e solicitações de suporte, permitindo sua categorização por severidade, impacto e prioridade, bem como a rastreabilidade integral das ações adotadas. Esses mecanismos deverão viabilizar a aferição objetiva da qualidade do suporte prestado, inclusive para fins de avaliação de desempenho, aplicação de acordos de níveis de serviço e responsabilização.
- 8.5.** Considerando a criticidade da Rede Governo, a solução deverá demonstrar capacidade de assegurar tempos máximos de atendimento compatíveis com ambientes de missão crítica, admitindo diferenciação conforme a severidade do incidente, o impacto sobre os serviços públicos suportados e a localização geográfica das unidades atendidas. Em especial, a solução deverá ser capaz de prover resposta tempestiva a ocorrências que impliquem indisponibilidade total ou degradação relevante dos serviços, inclusive com mobilização de suporte presencial quando tecnicamente necessário.
- 8.6.** A solução deverá, ainda, possibilitar a atualização contínua e controlada de seus componentes, incluindo correções de falhas, aplicação de patches de segurança, ajustes de configuração e adequações técnicas necessárias à preservação da integridade, da disponibilidade e da aderência às políticas institucionais de segurança da informação. Tais atualizações deverão ser realizadas de modo a minimizar impactos operacionais e riscos à estabilidade do ambiente.
- 8.7.** A arquitetura da solução deverá ser compatível com um modelo de gestão centralizada da manutenção e do suporte, permitindo o monitoramento contínuo do ambiente, a atuação proativa sobre eventos e a coordenação técnica das intervenções. Esse modelo deverá assegurar visibilidade integral sobre o funcionamento dos ativos, dos enlaces de conectividade e dos mecanismos de segurança, possibilitando a identificação antecipada de falhas e a adoção de ações corretivas antes da ocorrência de impactos relevantes aos serviços públicos.
- 8.8.** A solução deverá contemplar, ainda, a disponibilização de documentação técnica atualizada e mecanismos de transferência de conhecimento, de modo a assegurar a adequada capacitação das equipes responsáveis pela gestão institucional da Rede Governo, reduzindo riscos de dependência excessiva e assegurando a continuidade operacional ao longo do tempo.
- 8.9.** A CONTRATADA deverá prestar suporte técnico durante toda a vigência contratual, a partir do recebimento definitivo da solução pela CONTRATANTE, assegurando atendimento contínuo 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive em feriados e finais de semana, por meio de central de atendimento telefônico (0800 e/ou número local) e ambiente WEB para abertura e acompanhamento de chamados.
- 8.10.** A abertura de chamado deverá gerar número único de identificação, com registro da data e hora, que servirá como marco inicial para a contagem dos prazos de atendimento e solução. Todos os chamados e as

providências adotadas deverão ser registrados e mantidos em sistema próprio da CONTRATADA, cujo acesso deverá ser disponibilizado à CONTRATANTE para fins de acompanhamento, controle e auditoria.

- 8.11.** A CONTRATADA deverá designar gestor responsável pelo contrato de suporte, que atuará como ponto focal junto à CONTRATANTE para escalonamento de demandas, resolução de ocorrências críticas e tratamento de eventuais falhas no atendimento, bem como disponibilizar acesso ao ambiente WEB do fabricante para obtenção de arquivos, atualizações e drivers necessários à operação da solução.
- 8.12.** Por fim, os requisitos de manutenção e suporte deverão estar alinhados ao modelo de prestação de serviços continuados adotado pela Administração Pública Estadual, assegurando condições técnicas e operacionais que viabilizem a fiscalização, a aferição objetiva do desempenho da solução e a aplicação de mecanismos de responsabilização, sem prejuízo da continuidade, da estabilidade e da qualidade dos serviços prestados pela Rede Governo.

LOTE 02

- 8.13.** A solução a ser contratada deverá assegurar manutenção contínua e serviço de garantia técnica compatíveis com a criticidade dos serviços de segurança da informação utilizados pelos órgãos e entidades do Poder Executivo Estadual, observadas as especificações técnicas estabelecidas no caderno de especificações do projeto.
- 8.14.** Os serviços de licenciamento e atualização de funcionalidades deverão garantir, durante toda a vigência contratual, o acesso regular às atualizações disponibilizadas pelos fabricantes, incluindo bases de assinaturas, correções de segurança, aprimoramentos funcionais e atualizações de firmware, quando aplicável, de modo a preservar a efetividade dos mecanismos de proteção e a aderência tecnológica das soluções em uso.
- 8.15.** A contratada deverá assegurar a continuidade do serviço de garantia técnica técnico associado às soluções licenciadas, incluindo atendimento a demandas relacionadas a falhas de funcionamento, indisponibilidade de funcionalidades licenciadas, inconsistências de atualização e demais ocorrências que possam comprometer a operação regular dos mecanismos de segurança, respeitados os níveis de serviço e prazos definidos neste Termo de Referência.
- 8.16.** No caso da Solução de Segurança de Rede – Segmentação Interna – Tipo I, os requisitos de manutenção e garantia deverão contemplar a sustentação das funcionalidades de segmentação lógica do tráfego interno de rede, garantindo a atualização de componentes, a correção de eventuais vulnerabilidades e a preservação da compatibilidade com o ambiente tecnológico existente.
- 8.17.** A CONTRATADA deverá prestar serviço de garantia técnica durante toda a vigência contratual, a partir do recebimento definitivo da solução pela CONTRATANTE, assegurando atendimento contínuo 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive em feriados e finais de semana, por meio de central de atendimento telefônico (0800 e/ou número local) e ambiente WEB para abertura e acompanhamento de chamados.
- 8.18.** A abertura de chamado deverá gerar número único de identificação, com registro da data e hora, que servirá como marco inicial para a contagem dos prazos de atendimento e solução. Todos os chamados e as providências adotadas deverão ser registrados e mantidos em sistema próprio da CONTRATADA, cujo acesso deverá ser disponibilizado à CONTRATANTE para fins de acompanhamento, controle e auditoria.
- 8.19.** A CONTRATADA deverá designar gestor responsável pelo contrato de suporte, que atuará como ponto focal junto à CONTRATANTE para escalonamento de demandas, resolução de ocorrências críticas e tratamento de eventuais falhas no atendimento, bem como disponibilizar acesso ao ambiente WEB do fabricante para obtenção de arquivos, atualizações e drivers necessários à operação da solução.

9. LOCAL PARA ENTREGA E/OU EXECUÇÃO DOS BENS/SERVIÇOS

LOTE 1

9.1. Locais de Prestação dos Serviços – Lote 1

9.1.1. Os serviços serão executados para atendimento às unidades administrativas integrantes da Rede Governo, distribuídas em todo o território do Estado da Bahia, abrangendo capital, Região Metropolitana de Salvador e interior, inclusive em municípios que venham a ser incorporados à rede ao longo da vigência contratual. A execução deverá considerar a natureza distribuída da Rede Governo e a necessidade de atendimento contínuo às unidades em operação.

9.1.2. O modelo de execução deverá contemplar a atuação da contratada tanto de forma remota quanto presencial, conforme a natureza das atividades, a criticidade dos serviços e a localização geográfica das unidades atendidas, observada a classificação por macrorregiões e a existência de infraestrutura centralizada de monitoramento no Data Center da PRODEB, localizado em Salvador.

9.1.3. A CONTRATADA deverá atender todas as unidades governamentais localizadas no estado da Bahia, ciente de que poderá haver criação ou desativação de unidades, inclusive em municípios não previstos inicialmente.

9.1.4. As unidades estão classificadas conforme abaixo.

Centro de Monitoramento Integrado – Datacenter da PRODEB localizado em Salvador.

Macrorregião 01 – Salvador e localidades situadas até 50 km.

Macrorregião 02 – Localidades situadas entre 51 até 300 km de Salvador.

Macrorregião 03 – Localidades situadas acima de 300 km de Salvador.

9.1.5. Após a formalização e assinatura do contrato entre o ÓRGÃO CONTRATANTE e a CONTRATADA, o gestor deverá realizar o cadastramento do instrumento no portal da Rede Governo, disponibilizado pela PRODEB, incluindo suas informações principais e a cópia do documento;

9.1.5.1 Uma vez cadastrado e ativado, todas as solicitações de atendimento deverão ser realizadas exclusivamente por meio desse portal, mediante o registro de Ordem de Serviço, não se limitando a uma relação prévia ou estática de unidades, devendo o CONTRATANTE informar, a cada demanda, os dados da unidade a ser atendida, incluindo endereço, contatos dos responsáveis e demais informações necessárias à execução dos serviços de implantação, ampliação, mudança ou desativação, sendo tais informações automaticamente disponibilizadas à CONTRATADA,

9.1.5.2 A CONTRATADA deverá executar as atividades e manter o status das demandas atualizado no sistema, garantindo a rastreabilidade e a gestão centralizada de todo o fluxo de atendimento;

9.2. Horários de Prestação dos Serviços – Lote 1

9.2.1. A solução deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

9.2.2. A CONTRATADA deverá manter plantão técnico de suporte on-site 24x7, com escala formalmente estabelecida e informada ao CONTRATANTE, incluindo mecanismos para atendimento imediato de incidentes fora do horário comercial (08h00 às 18h00, de segunda a sexta-feira).

LOTE 2

9.3. Os serviços decorrentes da Ata de Registro de Preços serão executados predominantemente de forma remota, em razão de sua natureza vinculada ao licenciamento, à atualização e à manutenção de funcionalidades de soluções de segurança da informação, sem prejuízo de eventuais interações técnicas necessárias com os ambientes tecnológicos dos órgãos e entidades contratantes.

9.4. Quando tecnicamente justificado ou quando as características da atividade assim exigirem, os serviços poderão ser executados de forma presencial nas dependências do órgão ou entidade contratante, especialmente para atendimento de demandas que não possam ser adequadamente realizadas de maneira remota, observadas as condições e os limites estabelecidos nos instrumentos contratuais.

- 9.5.** A execução abrangerá os ambientes de tecnologia da informação e comunicação dos Órgãos e Entidades do Poder Executivo Estadual, onde se encontram implantadas as soluções de segurança objeto da contratação, bem como os ambientes centralizados de gestão, monitoramento, autenticação e relatoria, quando aplicável.
- 9.6.** Eventuais atividades presenciais ou que demandem interação direta com a infraestrutura dos Órgãos e Entidades deverão observar rigorosamente as diretrizes técnicas, operacionais e de segurança definidas pela Administração.

10. REQUISITOS DE TREINAMENTO – LOTE 01

- 10.1.** O serviço de treinamento a que se refere ao item 21 - Solução de Gestão, Operação e Monitoramento Central deste Termo de Referência, caso seja presencial, deverá ser executado na sede da CONTRATANTE, situada na Avenida 4, nº 410, Centro Administrativo da Bahia – CAB, Salvador, Bahia, CEP: 41.745-002.
- 10.2.** O serviço de treinamento a que se refere o item Solução de Gestão, Operação e Monitoramento Central deverá ser realizado presencialmente em dias úteis, obedecendo aos horários abaixo discriminados:
- 10.2.1. Segunda a quinta: 08:30hs às 12:00hs e das 14:00hs às 17:00hs;
- 10.2.2. Sexta: 08:30hs às 12:00hs e das 14:00hs às 15:00hs.
- 10.3.** A CONTRATADA deverá emitir certificados de conclusão do treinamento. Deverá constar no certificado a data de início e fim, carga horária, nome do instrutor, nome do treinamento e nome do participante;
- 10.4.** A CONTRATADA deverá apresentar, em até 20 (vinte) dias após assinatura do Contrato, um Plano de Treinamento que será avaliado e aprovado pela equipe técnica da CONTRATANTE;
- 10.5.** O Plano citado no item anterior deverá apresentar o programa de cada treinamento com conteúdo, carga horária, duração em dias, modalidade e avaliações de aprendizagem.
- 10.6.** O detalhamento deste item encontra-se no Anexo de Especificações Técnicas da Rede Governo, parte integrante deste Termo de Referência.

III. DA LICITAÇÃO

11. CONDIÇÕES DA ATA DE REGISTRO DE PREÇO

- 11.1.** As quantidades estabelecidas para cada um dos itens são estimativas e não constituem compromisso de demanda.
- 11.2.** A existência de preços registrados não obriga à realização de futuras contratações, sendo facultada à Administração a utilização de outros meios, respeitada a legislação relativa às licitações, sendo assegurada ao beneficiário do registro a preferência em igualdade de condições.
- 11.3.** A Ata de Registro de Preços poderá ser objeto de adesão por órgãos e entidades não participantes, nos termos do art. 86, § 2º, da Lei Federal nº 14.133/2021 e do Decreto Estadual nº 23.657/2025, desde que previamente autorizada pela Secretaria da Administração do Estado da Bahia – SAEB, em conformidade com o Termo de Cooperação Técnica, cabendo ao órgão gerenciador a análise e anuência quanto à disponibilidade de saldo, condições da Ata e viabilidade operacional, devendo ser observados os quantitativos registrados e as condições comerciais e técnicas estabelecidas no instrumento convocatório, no Termo de Referência e na Ata de Registro de Preços.
- 11.4.** A Companhia de Processamento de Dados do Estado da Bahia – PRODEB atuará como órgão gerenciador da Ata de Registro de Preços, sendo responsável pela sua gestão operacional, incluindo o controle de vigência, saldos e registros, ficando a utilização da Ata, para fins de contratação, saque ou adesão, condicionada à prévia e expressa autorização da Secretaria da Administração do Estado da Bahia – SAEB, nos termos do Termo de Cooperação Técnica firmado entre as partes.

11.5. As atas de registro de preços permanecerão abertas à adesão de órgãos e entidades não participantes, observado o interesse da Administração e os limites legais aplicáveis, caracterizando-se como atas passíveis de adesão. O órgão gerenciador poderá promover o remanejamento dos quantitativos registrados na Ata de Registro de Preços entre os órgãos e entidades participantes, observado o disposto na legislação aplicável e condicionado à prévia e expressa autorização da Secretaria da Administração do Estado da Bahia – SAEB.

11.6. As atas de registro de preços permanecerão abertas à adesão de órgãos e entidades não participantes, observado o interesse da Administração e os limites legais aplicáveis, caracterizando-se como atas passíveis de adesão.

11.7. As aquisições ou as contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o órgão ou a entidade gerenciadora e para os órgãos ou as entidades participantes, em conformidade com o art. 148, inciso I, do RLC e art. 41 do Decreto Estadual nº 23.657/2025.

11.8. Em observância ao art. 148 do RLC e art. 41 do Decreto Estadual nº 23.657/2025, o quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão ou a entidade gerenciadora e os órgãos ou as entidades participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

11.9. A estimativa das quantidades a serem contratadas foi elaborada com base em levantamento realizado por meio de consulta junto aos órgãos e entidades integrantes da Rede Governo, no período de 18 a 26 de dezembro de 2025. O levantamento foi operacionalizado pela Secretaria da Administração do Estado da Bahia – Saeb, mediante o preenchimento de formulário estruturado, no qual foram disponibilizados todos os itens previstos neste TR, com campos específicos para indicação das quantidades demandadas em cada um dos cinco anos de vigência contratual.

11.10. Caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente da adesão superveniente, desde que não prejudique as obrigações presentes e futuras decorrentes da ata.

11.11. Compete ao órgão não participante os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação de sanções, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações.

11.12. O edital deverá prever que a Ata de Registro de Preços terá vigência inicial de 01 (um) ano, podendo ser prorrogada por igual período, desde que comprovada a vantajosidade do preço, com renovação integral dos quantitativos para o novo período, conforme o art. 18 do Decreto Estadual nº 23.657/2025 e art. 137 do RLC da Prodeb.

11.13. Em caso de exclusão do primeiro colocado, da ata decorrente desse sistema de registro de preços, nas hipóteses previstas nos artigos 144 e 145 do Regulamento de Licitações e Contratos da Prodeb, apenas será possível sacar do segundo colocado, caso o mesmo tenha ofertado solução igual a ofertada pelo primeiro (hardwares/software dos mesmos fabricantes ou caso ainda não tenha sido realizado saque).

11.14. O instrumento convocatório contemplará minutas contratuais distintas, compatíveis com os regimes jurídicos aplicáveis, destinadas às contratações a serem firmadas pela PRODEB, eventualmente, pelas empresas estatais, e pelos órgãos e entidades da Administração Pública Direta, observados, respectivamente, o Regulamento de Licitações e Contratos da PRODEB e os modelos contratuais padronizados da Procuradoria Geral do Estado.

12. MODALIDADE DE LICITAÇÃO

12.1. Diante da natureza comum do objeto, o procedimento licitatório será realizado na modalidade pregão eletrônico, adotando-se como critério de julgamento o menor valor global por lote, em conformidade com o disposto nos arts. 6º, incisos XLI e XLV, 12, inciso VI, 29 e 33, inciso I, da Lei Federal nº 14.133/2021, bem como nos arts. 2º, 5º, parágrafo único, 6º e 7º, inciso I, do Decreto Estadual nº 22.888/2024, observada a compatibilização procedimental com o Regulamento de Licitações e Contratos da PRODEB, especialmente nos arts. 4º, inciso VI, 54, inciso IV, e 57, inciso I.

12.2. O critério de julgamento a ser adotado é o menor valor global por lote.

12.3. Considerando que os lotes contemplam diversos itens e, com o objetivo de evitar desequilíbrio na composição dos preços individuais por item, não serão aceitas propostas cujo valor global esteja dentro do limite máximo, mas não estejam cumprindo o limite máximo de cada item.

12.4. A licitação deverá ser processada em dois lotes conforme abaixo:

12.4.1. LOTE 01: Solução de conectividade segura, incluindo proteção de borda, firewall de próxima geração (NGFW) com tecnologia SD-WAN, links de internet e Solução de Gestão, Operação e Monitoramento Central, pelo período de 60 meses; Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço, conforme especificações técnicas detalhadas neste Termo de Referência.

A estruturação deste lote busca superar as dificuldades operacionais identificadas no arranjo atualmente vigente, notadamente aquelas decorrentes de atuação simultânea de múltiplos fornecedores e da segregação entre serviços de conectividade e solução de segurança, garantindo maior efetividade na gestão, fiscalização e resolução de incidentes. Dessa forma, embora a licitação esteja organizada em mais de um lote, os serviços que compõem o Lote 01 apresentam caráter complementar, interdependente e integrado, não sendo tecnicamente viável sua contratação de forma fracionada.

12.4.2. LOTE 02: Soluções de segurança da informação e cibersegurança, compreendendo licenciamento, atualização, suporte, manutenção e demais serviços associados, voltados à proteção dos ambientes tecnológicos, das comunicações de dados e das aplicações corporativas dos órgãos e entidades do Poder Executivo Estadual, pelo período de 12 meses, conforme especificações técnicas detalhadas neste Termo de Referência.

12.5. O serviço a ser contratado pode ser descrito de forma objetiva, com padrões de desempenho e qualidade passíveis de definição precisa, mediante especificações técnicas usuais de mercado, razão pela qual se enquadra como serviço comum.

12.6. O Certame adotará o modo de disputa aberto;

12.7. No intuito de evitar o oferecimento de lances com variação insignificante, os lances ofertados deverão observar intervalo mínimo de diferença de valores, aplicável tanto aos lances intermediários quanto à proposta que venha a cobrir a melhor oferta, no valor de R\$ 100.000,00 (cem mil reais) para o Lote 1 e de R\$ 1.000,00 (mil reais) para o Lote 2.

13. CRITÉRIOS DE ACEITABILIDADE DA PROPOSTA

13.1. Não serão admitidas as propostas que desobedeçam aos critérios dispostos na Lei Federal 14.133/2021, no Decreto Estadual nº 22.888/2024, observada a compatibilização procedimental com o Regulamento de Licitações e Contratos da PRODEB, em seu art. 83;

13.2. Não serão aceitas propostas cuja descrição do objeto ofertado contenha simplesmente a expressão genérica “CONFORME EDITAL”, “DE ACORDO COM O EDITAL” ou expressões genéricas similares que não especifiquem com exatidão o objeto ofertado, suas características e aderência ao edital;

13.3. Deverão estar inclusas no valor do suporte técnico, toda e qualquer despesa relativa ao deslocamento dos técnicos à instalação da CONTRATANTE, bem como os referentes a transporte, frete e seguro, não ocorrendo qualquer ônus adicional para a CONTRATANTE;

13.4. As propostas precisam conter a razão social do fornecedor, telefone para contato, endereço, preposto responsável, CNPJ, além de estarem devidamente assinadas e datadas;

13.5. As propostas deverão ter o seu prazo de validade não inferior a 60 (sessenta dias) dias da sua emissão;

13.6. Considerando as características técnicas e a criticidade dos objetos previstos nos Lotes 01 e 02, deverá ser apresentado, juntamente com a proposta, uma declaração para cada um dos lotes, fornecida pelo fabricante dos equipamentos, em papel timbrado, informando que a licitante é sua revenda e/ou assistência técnica autorizada, conferindo desta maneira mais segurança e confiabilidade na execução do objeto, conhecimento técnico e reposição de peças;

13.6.1. Lote 01 - A natureza deste lote exige integração plena entre conectividade, segurança, orquestração e gestão central, pois trata-se de uma solução tecnicamente unificada e indivisível, típica de arquiteturas modernas de redes governamentais distribuídas. Assim, para garantir que a implantação e a operação sejam conduzidas com segurança, confiabilidade e acesso às atualizações corretivas e evolutivas, é imprescindível que a licitante possua autorização formal do fabricante; tenha acesso legítimo ao suporte técnico oficial e capacidade reconhecida para configuração, escalabilidade e manutenção da solução ponta a ponta.

13.6.1.1 Considerando o disposto no item 2.1.1 – Base Implantada, e visando assegurar a continuidade operacional, a interoperabilidade e a integridade da arquitetura de segurança da informação atualmente em produção, a licitante deverá, no momento da apresentação da proposta, declarar expressamente a compatibilidade da solução ofertada com os equipamentos já existentes na infraestrutura da CONTRATANTE.

13.6.1.2 Caso a solução ofertada não seja plenamente compatível com os equipamentos atualmente utilizados pela PRODEB, a licitante deverá obrigatoriamente apresentar, juntamente com a proposta, toda a documentação técnica comprobatória dos equipamentos a serem fornecidos em substituição as soluções informados no item 2.1.1

13.6.1.3 A documentação técnica deverá comprovar, de forma inequívoca, que os equipamentos ofertados atendem, no mínimo, à mesma quantidade, capacidade, desempenho e funcionalidades dos equipamentos atualmente instalados na infraestrutura da CONTRATANTE, conforme descrito no item 2.1.1, sendo admitidas soluções de capacidade equivalente ou superior.

13.6.1.4 Deverão ser apresentados, para fins de análise de aceitabilidade da proposta, catálogos técnicos, datasheets, arquiteturas de referência, matrizes de compatibilidade, bem como demais documentos oficiais do fabricante que evidenciem o pleno atendimento aos requisitos técnicos e funcionais estabelecidos neste Termo de Referência.

13.6.1.5 O não atendimento ao disposto neste item, bem como a ausência ou insuficiência de comprovação técnica, implicará na desclassificação da proposta, por descumprimento dos critérios de aceitabilidade estabelecidos neste Edital.

13.6.2. O Lote 02 envolve Licenciamento e atualizações e serviços associados a soluções de segurança dos ambientes tecnológicos, comunicações de dados e aplicações corporativas, pelo período de 12 meses. Esses serviços dependem da conformidade técnica e contratual com o fabricante, pois somente empresas autorizadas possuem acesso às versões mais recentes de firmware e atualizações de segurança; habilitação para aplicar patches críticos; capacitação reconhecida para tratamento de incidentes de cibersegurança e garantia de integridade, autenticidade e rastreabilidade das soluções implementadas.

A ausência dessas comprovações criaria risco elevado de interrupção dos serviços, dificultando diagnósticos, reposição de peças, atendimento a incidentes e continuidade operacional.

13.7. Não serão aceitas propostas com valores unitário e global superiores ao estimado;

13.8. A não comprovação de qualquer dos itens acima implicará na imediata desclassificação da proponente;

13.9. A Proponente deverá apresentar manuais, documentos ou datasheets oficiais do fabricante, de domínio público, em língua portuguesa ou inglesa, devendo ser referenciado a página e o capítulo que comprova o seu atendimento (Planilha ponto a ponto), para cada um dos itens conforme tabela abaixo:

LOTE	ITEM	COMPROVAÇÕES PARA
Lote 01	Solução de Conectividade Segura	Firewall de Próxima Geração (NGFW)
	Solução de Operação e Monitoramento Central	Firewall de Próxima Geração (NGFW)
		Plataforma Centralizada de Gerenciamento de Dispositivos
		Solução de Zero Trust Access (ZTA)
	Solução de Monitoramento e Relatoria De Logs	Solução de Monitoramento e Relatoria De Logs
Lote 02	Solução De Segurança de Aplicações WAF	Solução De Segurança de Aplicações WAF
	Solução De Segurança de Rede NGFW	Solução De Segurança de Rede NGFW

14. QUALIFICAÇÃO TÉCNICA

14.1. Para fins de habilitação técnica, a licitante arrematante deve apresentar, na forma e nos prazos indicados no edital, documentos de comprovação quanto à capacidade técnico-operacional.

14.2. Os documentos devem ser apresentados em língua portuguesa, com a ressalva que serão aceitos documentos técnicos, e datasheets em língua inglesa devido à ausência de tradução das Terminologias Técnicas.

14.3. LOTE 1: A PROPONENTE deverá apresentar atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, comprovando que prestou serviços de Solução de conectividade segura, incluindo proteção de borda, firewall de próxima geração (NGFW) com tecnologia SD-WAN, links de internet e Solução de Operação e Monitoramento Central, incluindo instalação, configuração e suporte. É exigido que seja apresentado um ou mais atestados, cuja soma totalize pelo menos 20% (vinte por cento) do quantitativo total estimado.

14.3.1. A exigência de apresentação de atestado(s) de capacidade técnica prevista no item 14.4 justifica-se pela complexidade técnica, criticidade operacional e abrangência territorial da solução de conectividade segura, que envolve a prestação integrada de serviços de rede e segurança gerenciados a elevado número de unidades distribuídas geograficamente. Assim, mostra-se necessária a comprovação da capacidade técnico-operacional da licitante por meio de experiência prévia na execução de serviços semelhantes ou compatíveis em características e quantidades com o objeto da contratação, em escala suficiente para mitigar riscos de inexecução contratual, admitindo-se a apresentação de um ou mais atestados que evidenciem tal aptidão, nos termos definidos neste Termo de Referência.

14.4. LOTE 2: A PROPONENTE deverá apresentar atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, comprovando que prestou serviços solução de segurança da informação e cibersegurança, compreendendo licenciamento, atualização e garantia. É exigido que seja apresentado um ou mais atestados, cuja soma totalize pelo menos 20% (vinte por cento) do quantitativo total estimado.

- 14.4.1. O percentual de 20% (vinte por cento) se justifica para comprovar a capacidade técnico-operacional da licitante para o desempenho de atividade pertinente e compatível em características e quantidades com o objeto da licitação, mitigando assim, os riscos de inexecução do contrato.

LOTE	Descritivo dos Itens	QTD Total (100%)	Comprovação (20%)
LOTE 01	Solução de Conectividade Segura com NGFW e Link de Internet - Incluindo instalação, configuração, sustentação e suporte técnico durante a vigência contratual, com características técnicas semelhantes às especificadas neste Termo de Referência	4571	914
LOTE 02	Solução De Segurança de Aplicações WAF	12	02
	Solução De Segurança de Rede Ambiente Híbridos	10	02
	Solução De Segurança de Rede Segmentação Interna	154	30

- 14.5.** Todas as informações citadas acima deverão constar de forma explícita no(s) atestado(s).
- 14.6.** A proposta da licitante deverá vir acompanhada de documentação técnica que comprove o atendimento dos requisitos, incluindo os datasheets dos equipamentos.
- 14.7.** É preferível que os atestados emitidos por pessoa jurídica de direito privado contenham assinatura digital certificada ou com reconhecimento de firma, que assegure sua autenticidade. Caso a assinatura do responsável técnico não contenha elemento de autenticação, a Prodeb se resguarda ao direito de realizar diligência para solicitar documentos a fim de sanar eventuais dúvidas quanto ao referido atestado.
- 14.8.** A CONTRATANTE se reserva o direito de conferir as informações prestadas pelas empresas emitentes dos atestados, através de consultas e visitas, bem como a disponibilidade de equipamentos solicitados junto à PROPONENTE.
- 14.9.** A LICITANTE deverá apresentar relação explícita e declaração formal de disponibilidade dos recursos humanos e materiais necessários, sob as penas da lei, especialmente o disposto no art. 155, inc. VIII, da Lei nº 14.133/2021 e art. 211 do RLC da Prodeb.
- 14.10.** Deverá ser apresentado profissionais técnicos pertencentes ao quadro da empresa — sócios, empregados ou prestadores de serviços — devidamente capacitados pelo fabricante para realizar a instalação, configuração e manutenção dos itens ofertados, com comprovação por certificados de qualificação vigentes emitidos pelo fabricante, conforme quantitativos abaixo:

LOTE	Descrição da Certificação	QTD Total
LOTE 01	Certificação de Solução de Gestão e Relatoria de Logs	01
	Certificação de NGFW e ou SDWAN para Solução de Conectividade Segura.	10
	Certificação de Plataforma Centralizada de Gerenciamento de Dispositivos.	01
	Certificação de Solução de Zero Trust Access.	02
	Certificação em ITIL Foundation Certificate in IT Service Management	01

	Diploma de Pós-graduação e ou MBA em Gestão de Projetos	02
LOTE 02	Certificação de Solução De Segurança de Aplicações WAF.	01
	Certificação de Solução de Rede NGFW	03

14.11. Além das certificações descritas na tabela acima, a licitante deverá comprovar que ao menos 01 (um) profissional possui registro profissional ativo no respectivo conselho competente (CREA ou CFT), compatível com as atribuições técnicas inerentes ao objeto contratado.

14.12. A relação dos profissionais técnicos deverá estar acompanhada de comprovação de vínculo com a licitante, mediante a apresentação de, no mínimo, um dos seguintes documentos, conforme o caso:

14.12.1. CTPS;

14.12.2. Contrato social;

14.12.3. Contrato de prestação de serviços;

14.12.4. Termo de compromisso de integração ao quadro técnico no caso de adjudicação.

14.13. Os profissionais indicados deverão participar efetivamente da execução contratual, sendo admitida substituição apenas por profissionais de experiência equivalente ou superior, com anuência da Administração.

15. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

15.1. A licitante deverá apresentar certidão negativa de falência expedida pelo distribuidor da sede do licitante, com data de expedição ou revalidação dos últimos 90 (noventa) dias anteriores à data da realização da licitação, caso o documento não consigne prazo de validade;

15.2. A licitante deverá apresentar índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante);

Solvência Geral (SG) = Ativo Total / (Passivo Circulante + Passivo Não Circulante);

Liquidez Corrente (LC) = Ativo Circulante / Passivo Circulante.

15.2.1. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) ou Liquidez Corrente (LC), será exigido, para fins de habilitação econômico-financeira, patrimônio líquido mínimo correspondente a 10% (dez por cento) do valor estimado da contratação, devendo a comprovação observar, como base de cálculo, o valor estimado fixado pela PRODEB, e não o valor final da proposta apresentada pelo licitante.

15.2.2. O balanço patrimonial, a demonstração do resultado do exercício e as demais demonstrações contábeis limitar-se-ão ao último exercício, caso a pessoa jurídica tenha sido constituída há menos de 2 (dois) anos, nos termos do art. 69, §6º, da Lei Federal nº 14.133/2021.

15.2.3. O balanço patrimonial e as demonstrações contábeis poderão ser atualizados por índices oficiais quando encerrados há mais de 3 (três) meses da data da apresentação da proposta, vedada a sua substituição por balancetes ou balanços provisórios.

15.2.4. O licitante apresentará o balanço patrimonial e a demonstração do resultado do exercício mediante, conforme o caso, publicação em Diário Oficial ou jornal de grande circulação, registro na Central de Balanços no âmbito do Sistema Público de Escrituração Digital – SPED, ou cópia reprográfica das páginas do Livro Diário, com os respectivos Termos de Abertura e Encerramento registrados na Junta Comercial.

- 15.2.5. O atendimento dos índices econômicos previstos neste subitem será atestado mediante declaração assinada por profissional legalmente habilitado da área contábil, apresentada pelo licitante, nos termos do art. 69, §1º, da Lei Federal nº 14.133/2021.
- 15.2.6. Na hipótese de participação de empresas reunidas em consórcio, **conforme previsto para o Lote 01**, a verificação dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC) será realizada com base nos valores consolidados, obtidos pela soma dos ativos e passivos correspondentes das empresas consorciadas, vedada a simples soma ou média dos índices individuais.
- 15.2.6.1. A título exemplificativo, considerando um consórcio composto por duas empresas, sendo a Empresa A com Ativo Circulante de R\$ 20.000.000,00 (vinte milhões de reais), Realizável a Longo Prazo de R\$ 10.000.000,00 (dez milhões de reais), Passivo Circulante de R\$ 15.000.000,00 (quinze milhões de reais) e Passivo Não Circulante de R\$ 5.000.000,00 (cinco milhões de reais), e a Empresa B com Ativo Circulante de R\$ 30.000.000,00 (trinta milhões de reais), Realizável a Longo Prazo de R\$ 20.000.000,00 (vinte milhões de reais), Passivo Circulante de R\$ 25.000.000,00 (vinte e cinco milhões de reais) e Passivo Não Circulante de R\$ 10.000.000,00 (dez milhões de reais), o cálculo do Índice de Liquidez Geral (LG) deverá considerar os valores consolidados do consórcio. Nesse caso, o Ativo Circulante consolidado será de R\$ 50.000.000,00 (cinquenta milhões de reais), o Realizável a Longo Prazo consolidado de R\$ 30.000.000,00 (trinta milhões de reais), o Passivo Circulante consolidado de R\$ 40.000.000,00 (quarenta milhões de reais) e o Passivo Não Circulante consolidado de R\$ 15.000.000,00 (quinze milhões de reais), resultando em Índice de Liquidez Geral (LG) igual a 1,45, obtido pela aplicação da fórmula prevista no item 16.2.
- 15.2.7. Na hipótese de participação de empresas reunidas em consórcio, caso o resultado apurado de forma consolidada seja inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) ou Liquidez Corrente (LC), será exigido, para fins de habilitação econômico-financeira, o patrimônio líquido mínimo correspondente ao percentual previsto no item 16.1, observado que, quando o consórcio não for formado integral ou exclusivamente por microempresas ou empresas de pequeno porte, o referido percentual será acrescido de 10% (dez por cento) em relação ao exigido para os licitantes individuais.
- 15.2.7.1. A título exemplificativo, considerando uma contratação cujo valor estimado seja de R\$ 100.000.000,00 (cem milhões de reais), o patrimônio líquido mínimo exigido nos termos do item 15.2.1 corresponderá a R\$ 10.000.000,00 (dez milhões de reais). Na hipótese de participação de consórcio não formado integral ou exclusivamente por microempresas ou empresas de pequeno porte, e verificada a necessidade de comprovação de patrimônio líquido mínimo nos termos do item 15.2.7, o valor exigido será acrescido de 10% (dez por cento), totalizando R\$ 11.000.000,00 (onze milhões de reais), podendo tal montante ser comprovado de forma consolidada pela soma dos patrimônios líquidos das empresas consorciadas.

16. SUBCONTRATAÇÃO

LOTE 01

- 16.1.** Será admitida a subcontratação limitada exclusivamente ao fornecimento de links de comunicação de dados, parte integrante do Lote 01, como parcela acessória e instrumental da solução, porquanto não há comprometimento da governança, da segurança e da responsabilidade técnica global da CONTRATADA, restando claro e patente que o CONTRATANTE não se responsabiliza por nenhum compromisso assumido pela CONTRATADA perante terceiros.
- 16.2.** Entende-se como escopo principal do objeto o conjunto de itens para os quais, como requisito de habilitação técnico – operacional, foi exigida a apresentação de atestados que comprovem a execução de serviço com características semelhantes – transporte de dados, camadas essenciais de gestão, controle, segurança da informação, monitoramento, disponibilidade, desempenho e integração operacional, haja vista que caracterizam o núcleo crítico da solução e não poderão ser objeto de subcontratação, devendo permanecer sob a responsabilidade direta, integral e exclusiva da CONTRATADA.

16.3. Em caso de subcontratação, sempre que possível, a Contratada deverá priorizar a subcontratação de microempresa (ME) ou empresa de pequeno porte (EPP) para executar parcela do objeto, nos termos do art. 48, inc. II, da Lei Complementar nº 123/2006.

16.4. A CONTRATADA deve submeter à apreciação da CONTRATANTE o pedido de prévia anuência para subcontratação, com apresentação do pretendente subcontratado e da respectiva documentação, que deve corresponder à exigida para habilitar nesta licitação.

16.5. A documentação apresentada será analisada pela CONTRATANTE, incluindo parecer técnico da fiscalização, ao qual cabe avaliar se a subcontratada cumpre os requisitos de qualificação técnica necessários para a execução do serviço.

16.6. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da CONTRATADA pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante a CONTRATANTE pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

16.7. É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

16.8. Nos casos de subcontratação autorizada, não será admitida a emissão de notas fiscais pelas empresas subcontratadas, devendo todo o faturamento decorrente da execução contratual ser realizado exclusivamente em nome da empresa contratada, que permanecerá como única responsável perante a CONTRATANTE pela integral execução do objeto, pelo cumprimento dos níveis de serviço, pela qualidade das entregas, pela segurança da informação e pela continuidade operacional da Rede Governo.

16.9. A CONTRATANTE não aceitará, sob nenhum pretexto, a transferência de responsabilidade da CONTRATADA para outras entidades, sejam fabricantes, técnicos ou subcontratadas.

LOTE 02

16.10. Não será admitida a subcontratação do objeto contratual referente ao Lote 02.

17. CONSÓRCIO

LOTE 01

17.1. Para o lote 01 será permitida a participação de pessoas jurídicas reunidas em consórcio, considerando o elevado vulto, a complexidade técnica, a abrangência territorial e a essencialidade dos serviços objeto da contratação, como forma de viabilizar a conjugação de capacidades técnicas, operacionais e econômico-financeiras compatíveis com a adequada execução contratual, sem prejuízo da mitigação dos riscos associados.

17.2. A previsão de participação de pessoas jurídicas em consórcios no edital atende simultaneamente às disposições da Lei Federal nº 14.133/2021, da Lei Estadual nº 14.634/2023 e do Regulamento de Licitações e Contratos da PRODEB, não configurando indevida mistura de regimes jurídicos, mas sim compatibilização normativa legítima, adequada ao porte, ao risco e à relevância estratégica da contratação.

17.3. Poderão participar do certame as pessoas jurídicas reunidas em consórcio, constituído especificamente para executar o objeto desta licitação, limitado a três participantes, vedado ao consorciado competir isoladamente ou através de mais de um consórcio, devendo ser observado o disposto no Regulamento de Licitações e Contratos RLC da PRODEB e as seguintes regras:

17.3.1. As empresas consorciadas deverão apresentar, juntamente com os documentos de habilitação jurídica, a comprovação de compromisso público ou particular de constituição de consórcio, subscrito por todas as consorciadas, no qual deverão constar, no mínimo, os seguintes elementos:

- a) nome do consórcio;
- b) identificação completa de todas as empresas consorciadas, incluindo a razão social, CNPJ e endereço;
- c) indicação da composição do consórcio, com a informação do percentual/cota de participação de cada uma das consorciadas e suas funções e obrigações gerais no consórcio;
- d) indicação da empresa líder, responsável pelo consórcio, que deverá atender às condições de liderança, obrigatoriamente fixadas neste edital (art. 104, II do RLC da PRODEB);
- e) outorga à empresa líder de poderes expressos, irretratáveis e irrevogáveis, para representar o consórcio perante a PRODEB e a Administração Pública, em todas as fases da licitação e da execução do contrato dela eventualmente decorrente, facultando-lhe, inclusive, interpor e desistir de recursos, receber e dar quitação, comprometer-se a assinar, em nome do consórcio, quaisquer papéis e documentos relacionados com o objeto da licitação, firmar contratos e praticar todos os atos necessários visando à perfeita execução do objeto do contrato, bem como para receber citação e responder administrativa e/ou judicialmente pelas demais consorciadas;
- f) previsão da responsabilidade individual e solidária das consorciadas por todas as exigências do instrumento convocatório e as de ordem fiscal e administrativa, bem como pelos atos praticados em consórcio, tanto na fase de licitação quanto na de execução do eventual contrato dela decorrente, até o recebimento definitivo do objeto (art. 104, V do RLC da PRODEB);
- g) previsão da obrigação de efetiva constituição e registro do consórcio anteriormente à celebração do contrato resultante da licitação, na hipótese de as consorciadas sagrarem-se vencedoras (art.104, §2º, do RLC da PRODEB);
- h) prazo estipulado para a duração do consórcio, que deverá compreender todo o período de vigência do contrato até a aceitação definitiva do objeto licitado;
- i) previsão de que o consórcio não terá a sua constituição ou composição alterada sem a prévia e expressa anuência do órgão ou entidade contratante, até o cumprimento do objeto da licitação com a aceitação definitiva do objeto licitado (art. 104, § 4º, do RLC da PRODEB).

17.3.2. Caberá à empresa líder a apresentação dos documentos de representação do consórcio perante a PRODEB, nos termos do instrumento de constituição ou compromisso de consórcio.

17.3.3. No consórcio entre empresas brasileiras e estrangeiras, a liderança caberá, obrigatoriamente, à empresa brasileira, observado o disposto no art. 104, § 1º, do RLC da PRODEB).

17.3.4. Cada uma das empresas consorciadas deverá apresentar, de forma individualizada, a documentação exigida neste instrumento convocatório para a habilitação, nos termos do art. 104, inciso III, do RLC da PRODEB.

17.3.5. Para efeito de qualificação técnica, considerar-se-á o somatório dos quantitativos de cada consorciado, observado, entretanto, que o consorciado qualificado deve ser responsável pela prestação dos serviços a que se refira a qualificação computada na licitação, nos termos do art. 104, inciso III, do RLC da PRODEB.

17.3.6. As empresas consorciadas respondem individual e solidariamente pelos atos praticados pelo consórcio, tanto na fase da licitação quanto na de execução do contrato dela decorrente, até o recebimento definitivo do objeto (art. 104, inciso V, do RLC da PRODEB).

- 17.3.7. As empresas consorciadas, vencedoras da licitação, deverão providenciar, antes da celebração do contrato, a constituição definitiva do consórcio, em conformidade com o Termo de Compromisso de Constituição de Consórcio, devendo promover o arquivamento do instrumento próprio no órgão de registro correspondente ao da sede da empresa líder, nos termos do art. 104, §2º, do RLC da PRODEB. O não cumprimento dessa obrigação acarretará as consequências administrativas cabíveis, na forma do art. 155 da Lei nº 14.133/2021.
- 17.3.8. As empresas consorciadas não poderão alterar a constituição ou a composição do consórcio sem a prévia e expressa anuência do órgão contratante, até o cumprimento do objeto da licitação com o recebimento definitivo (art. 104, §4º do RLC da PRODEB).
- 17.3.9. O consórcio firmado deverá relacionar-se com o objeto da licitação, não sendo permitida a participação de pessoas ou empresas que não apresentem a necessária aptidão, na forma do disposto no respectivo ato convocatório. (art. 104, §3º do RLC da PRODEB).
- 17.3.10. A participação de empresas em consórcio é admitida pela Lei nº 14.133/2021, facultando à Administração estabelecer condições específicas no edital, desde que devidamente motivadas, inclusive quanto à fixação de limite máximo de empresas consorciadas, nos termos do art. 15, §4º, que exige justificativa técnica aprovada pela autoridade competente. Nesse contexto, a limitação do número de participantes do consórcio em até 03 (três) empresas mostra-se adequada e proporcional, considerando que consórcios excessivamente numerosos elevam a complexidade de governança, dificultam a coordenação operacional, ampliam os riscos de conflitos internos e comprometem a efetividade da responsabilidade solidária dos consorciados na execução contratual.

Adicionalmente, a restrição proposta contribui para a eficiência da execução e da fiscalização contratual, ao permitir melhor definição de responsabilidades e maior controle por parte da Administração, especialmente em contratações de natureza tecnológica que exigem elevado grau de integração técnica e operacional. Ressalta-se, ainda, que a medida não compromete a competitividade do certame, pois preserva a possibilidade de associação entre empresas para complementação de capacidades, ao mesmo tempo em que evita a formação de consórcios excessivamente amplos que possam, na prática, reduzir a concorrência.

LOTE 02

- 17.4.** Será vedada a participação de empresas reunidas em consórcio, tendo em vista que o objeto em contratação consiste em soluções padronizadas de segurança da informação e cibersegurança, abrangendo licenciamento, atualização, suporte, manutenção e demais serviços associados, vinculados à continuidade de uma arquitetura tecnológica já estabelecida no âmbito do Poder Executivo Estadual. Por se tratar de serviços homogêneos e integrados, cuja execução demanda atuação de uma única empresa especializada, não se verifica diversidade ou complexidade que justifique a formação de consórcios

IV. DO PAGAMENTO

18. FORMA DE PAGAMENTO

- 18.1.** Lote 1: Os serviços previstos nos itens 18, 19, 20 e 25 serão realizados sob demanda, mediante registro de Ordem de Serviço (OS), e pagos à vista, após a homologação pela CONTRATANTE, conforme previsto neste termo de referência.
- 18.1.1. Para todos os demais itens, os pagamentos serão realizados em 60 (sessenta) parcelas mensais, devendo a fatura ser emitida em até 10 (dez) dias úteis do mês subsequente ao da execução dos serviços, conforme previsto neste Termo de Referência.
- 18.2.** Lote 2: O fornecimento das licenças inclui a respectiva garantia, e o pagamento será realizado, a vista, após o recebimento definitivo, conforme previsto neste termo de referência.

18.3. A forma de pagamento das contratações decorrentes das atas de registro de preços observará o regime jurídico aplicável a cada ente contratante, bem como as condições e os prazos definidos nos respectivos instrumentos contratuais, conforme disposto a seguir.

18.4. Órgãos e Entidades da Administração Pública Direta

18.4.1. Para as contratações realizadas pelos órgãos e entidades da Administração Pública Direta do Poder Executivo Estadual, o pagamento será efetuado após a liquidação da despesa, observados os procedimentos e prazos estabelecidos no Termo de Referência.

18.4.2. Recebida a nota fiscal ou instrumento de cobrança equivalente, a Administração adotará as providências necessárias à liquidação da despesa no prazo de até 10 (dez) dias úteis, prorrogáveis por igual período, quando devidamente justificado, nos termos previstos no Termo de Referência.

18.4.3. Concluída a liquidação, o pagamento será realizado no prazo de até 05 (cinco) dias úteis, contados da finalização dessa etapa, mediante ordem bancária ou crédito em conta corrente da contratada, condicionado ao regular recebimento definitivo do objeto e ao ateste da execução contratual pelo fiscal competente.

18.4.4. Na hipótese de inconsistências na execução do objeto ou na documentação fiscal apresentada, o prazo para pagamento ficará suspenso até a devida regularização, reiniciando-se sua contagem sem ônus para a Administração, conforme disciplinado no Termo de Referência.

18.5. Companhia de Processamento de Dados do Estado da Bahia – PRODEB

18.5.1. Os prazos para pagamento observarão o disposto no art. 10 do Regulamento de Licitações e Contratos da PRODEB, de acordo com o valor contratado, a saber:

- i. Até R\$ 50.000,00: pagamento em até 15 (quinze) dias;
- ii. De R\$ 50.000,01 a R\$ 100.000,00: pagamento em até 30 (trinta) dias;
- iii. Acima de R\$ 100.000,01: pagamento em até 45 (quarenta e cinco) dias.

18.5.2. Os pagamentos estarão condicionados ao regular recebimento e aceite do objeto, bem como ao cumprimento das obrigações fiscais, trabalhistas e contratuais assumidas pela contratada.

18.5.3. O pagamento somente será autorizado depois de efetuado o “atesto” pela comissão ou servidor competente da CONTRATANTE na nota fiscal apresentada.

18.5.4. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

18.5.5. Antes da realização do pagamento deverá ser comprovada pela CONTRATADA a manutenção das condições de habilitação exigidas no edital e RLC da PRODEB.

18.5.6. A proposta e a nota fiscal de faturamento do bem e/ou serviço deverá refletir o objeto contratado. Sendo necessário o detalhamento da composição do objeto, esse deverá ser detalhado na proposta apresentada pelo proponente e reproduzido integralmente na respectiva nota fiscal.

18.5.7. A CONTRATADA deverá enviar as notas fiscais e documentos relacionados ao pagamento para o email: cofic.financeiro@prodeb.ba.gov.br.

18.6. O pagamento ficará condicionado à comprovação da prestação regular do serviço correspondente a cada item contratado, incluindo a efetiva disponibilização da conectividade segura, a manutenção da operação e o atendimento aos requisitos de desempenho e qualidade estabelecidos. A aferição da execução será realizada de forma periódica, com base em registros de ativação, relatórios operacionais e informações produzidas pelos mecanismos de monitoramento adotados pela Administração.

18.7. O cumprimento dos níveis mínimos de serviço, bem como a ocorrência de eventuais não conformidades, impactará o valor devido no período de apuração, mediante aplicação de descontos conforme detalhado neste Termo de Referência.

19. JUSTIFICATIVA DE PREÇO

19.1. O orçamento estimado para o objeto descrito e quantificado neste Termo de Referência corresponde ao valor máximo aceitável para a contratação e será alvo de publicidade na licitação pretendida, nos termos do art. 46 do Regulamento de Licitações e Contratos – RLC da PRODEB.

19.1.1. As planilhas de quantitativos estimados e dos preços unitários encontram-se acostados ao presente Termo de Referência como ANEXO III.

19.1.2. A estimativa de custos levou em consideração o risco envolvido na contratação e sua alocação entre CONTRATANTE e CONTRATADO, conforme especificado na matriz de risco que constitui ANEXO deste TR.

20. ADEQUAÇÃO ORÇAMENTÁRIA

A indicação da dotação orçamentária fica postergada para o momento da assinatura do(s) contrato(s) ou instrumento(s) equivalente(s), considerando tratar-se de procedimento licitatório para implantação de Sistema de Registro de Preços, nos moldes do Regulamento de Licitações e Contratos – RLC/PRODEB (art. 132, §4º) e do Decreto Estadual nº 23.657/2025 (art. 11).

V. DO CONTRATO

21. VIGÊNCIA DO CONTRATO

21.1. Lote 1

21.1.1 Para órgãos e entidades da Administração Pública direta, autárquica e fundacional do Poder Executivo Estadual – O prazo de vigência do contrato decorrente da ATA, a contar da data da sua assinatura, será de 05 (cinco) anos, considerando a natureza dos serviços contínuos, e a maior vantagem econômica para a Administração em razão da contratação plurianual prevista; podendo ser prorrogado até o limite de 10 (dez) anos, desde que atestada a vantajosidade econômica e a regularidade fiscal/trabalhista da contratada, nos termos do art. 107 da Lei nº 14.133/2021.

21.1.2 Para a PRODEB e demais empresas públicas e sociedades de economia mista integrantes da Administração Pública indireta - O prazo de vigência do contrato decorrente da ATA, a contar da data da sua assinatura, será de 05 (cinco) anos, nos termos do artigo 160 do RLC/PRODEB, e do artigo 71 da Lei Federal nº 13.303/2016, não sendo passível de renovação.

21.2. Lote 2: O prazo de vigência dos contratos decorrentes da Ata, a contar da data da sua assinatura, será de 12 (doze) meses, podendo ser prorrogados, por sucessivo (s) período (s), até atingir o limite de 05 (cinco) anos, nos termos do art. 160 do Regulamento de Licitações e Contratos da PRODEB e art. 106 da Lei Federal nº 14.133/2021.

22. OBRIGAÇÕES DA CONTRATADA

22.1. Zelar pelo cumprimento do objeto e das demais cláusulas deste Termo de Referência e Contrato;

22.2. Prestar os serviços, objeto deste Termo de Referência, com qualidade, eficiência, presteza, pontualidade e de forma ininterrupta, em conformidade com os termos e prazos estabelecidos;

22.3. Atender às solicitações de serviços de acordo com as especificações técnicas, cronogramas e condições especificadas;

22.4. Prestar os serviços com pessoal adequadamente capacitado em locais e instalações de acordo com as orientações constantes neste TR;

- 22.5.** Dispor de pessoal necessário para garantir a execução dos serviços, nos regimes contratados, sem interrupção seja por motivo de férias, descanso semanal, licença, falta ao serviço, greve, demissão e outros análogos, obedecidas às disposições da legislação trabalhista vigente;
- 22.6.** Não veicular publicidade ou qualquer outra informação acerca das atividades objeto deste contrato, sem prévia autorização da CONTRATANTE;
- 22.7.** Manter, durante a vigência do contrato, todas as condições de habilitação e qualificação exigidas neste TR;
- 22.8.** Assumir todas as providências e obrigações estabelecidas nas normas de segurança e legislação específica de acidentes de trabalho quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços ou em conexão com eles, ainda que verificadas nas dependências da CONTRATANTE;
- 22.9.** Assumir todas as despesas e ônus relativos ao seu pessoal, ficando ainda, para todos os efeitos legais, expressos pela CONTRATADA, a inexistência de qualquer vínculo empregatício entre seus empregados e/ou prepostos do CONTRATANTE;
- 22.10.** Acompanhar o cumprimento dos serviços cabendo-lhe integralmente o ônus decorrente de fiscalizá-los, não se eximindo das suas obrigações, independente das ações de fiscalização exercidas pela CONTRATANTE;
- 22.11.** Dar ciência a CONTRATANTE, imediatamente e por escrito, de qualquer anormalidade identificada na execução dos serviços, bem como as providências tomadas para a sua solução;
- 22.12.** Assumir total responsabilidade pelo sigilo das informações, dados, contidos em quaisquer mídias e documentos que seus empregados ou prepostos vierem a obter em função dos serviços prestados, mesmo após o término do prazo de vigência ou eventual rescisão do Contrato, respondendo pelos danos que eventual vazamento de informação, decorrentes de ação danosa ou culposa, nas formas de negligência, imprudência ou imperícia, venha a ocasionar a CONTRATANTE ou a terceiros;
- 22.13.** Responsabilizar-se pelo perfeito funcionamento do objeto do contrato, arcar com os eventuais prejuízos causados à Contratante e/ou a terceiros, provocados por ineficiência ou irregularidade cometida por seus empregados ou prepostos envolvidos na execução dos serviços, respondendo integralmente pelo ônus decorrente de sua culpa ou dolo na entrega dos serviços, o que não exclui nem diminui a responsabilidade pelos danos que se constatarem, independentemente do controle e fiscalização exercidos pela Contratante;
- 22.14.** Reparar, exclusivamente às suas custas, todos os defeitos, erros, falhas, omissões e quaisquer irregularidades verificadas na oferta de serviços, bem como responsabilizar-se por qualquer dano ou prejuízo daí decorrente;
- 22.15.** Garantir o atendimento dos prazos previstos nos Acordos de Nível de Serviço, sem prejuízo aos demais serviços, sempre que houver a necessidade de execução de correções em serviços já entregues;
- 22.16.** Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o CONTRATADO deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:
- 22.16.1. prova de regularidade relativa à Seguridade Social;
- 22.16.2. certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;
- 22.16.3. certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do CONTRATADO;
- 22.16.4. Certidão de Regularidade do FGTS – CRF; e
- 22.16.5. Certidão Negativa de Débitos Trabalhistas – CNDT.
- 22.17** Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

- 22.18.** Receber e dar o tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho.
- 22.19.** Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação;
- 22.20.** Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas.

23. PROTEÇÃO DE DADOS PESSOAIS

- 23.1.** As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.
- 23.2.** A CONTRATADA obriga-se a implementar medidas técnicas e administrativas suficientes visando a segurança, a proteção, a confidencialidade e o sigilo de toda informação, dados pessoais e/ou base de dados a que tenha acesso a fim de evitar acessos não autorizados, acidentes, vazamentos acidentais ou ilícitos que causem destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento não previstos.
- 23.3.** A CONTRATADA deve assegurar-se de que todos os seus colaboradores, consultores e/ou prestadores de serviços que, no exercício das suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, respeitem o dever de proteção, confidencialidade e sigilo.
- 23.4.** A CONTRATADA não poderá utilizar-se de informação, dados pessoais e/ou base de dados a que tenha acesso, para fins distintos ao cumprimento do objeto deste instrumento contratual.
- 23.5.** A CONTRATADA não poderá disponibilizar e/ou transmitir a terceiros, sem prévia autorização escrita, informação, dados pessoais e/ou base de dados a que tenha acesso em razão do cumprimento do objeto deste instrumento contratual.
- 23.6.** A CONTRATADA obriga-se a fornecer apenas a informação, dados pessoais e/ou base de dados estritamente necessários quando da transmissão autorizada a terceiros durante o cumprimento do objeto descrito neste instrumento contratual.
- 23.7.** A CONTRATADA fica obrigada a excluir ou devolver, a critério da contratante, todos os documentos, registros e cópias que contenham informação, dados pessoais e/ou base de dados a que tenha tido acesso durante a execução do objeto deste instrumento contratual no prazo de 30 (trinta) dias corridos, contados da data da ocorrência de qualquer uma das hipóteses de extinção do contrato, restando autorizada a conservação apenas nas hipóteses legalmente previstas.
- 23.8.** À CONTRATADA não será permitido deter cópias ou backups, informação, dados pessoais e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual.
- 23.9.** A CONTRATADA deverá eliminar os dados pessoais a que tiver conhecimento ou posse em razão do cumprimento do objeto deste instrumento contratual tão logo não haja mais necessidade de realizar seu tratamento.
- 23.10.** A CONTRATADA deverá notificar imediatamente a CONTRATANTE em caso de vazamento ou perda parcial ou total de informação, dados pessoais e/ou base de dados.
- 23.11.** A notificação não eximirá A CONTRATADA das obrigações e/ou sanções que possam incidir em razão da perda de informação, dados pessoais e/ou base de dados.
- 23.12.** A CONTRATADA que descumprir os termos da Lei nº 13.709/2018 suas alterações e regulamentações posteriores, durante ou após a execução do objeto descrito no presente instrumento contratual fica obrigada a assumir total responsabilidade e ao ressarcimento por todo e qualquer dano e/ou prejuízo sofrido, incluindo sanções aplicadas pela autoridade competente.

- 23.13.** A CONTRATADA fica obrigada a manter preposto para comunicação com CONTRATANTE para os assuntos pertinentes à Lei nº 13.709/2018 suas alterações e regulamentações posteriores.
- 23.14.** O dever de sigilo e confidencialidade, e as demais obrigações descritas na presente cláusula, permanecerão em vigor após a extinção das relações entre A CONTRATADA e a CONTRATANTE, bem como, entre A CONTRATADA e os seus colaboradores, subcontratados, consultores e/ou prestadores de serviços sob pena das sanções previstas na Lei nº 13.709/2018, suas alterações e regulamentações posteriores, salvo decisão judicial contrária.
- 23.15.** O não cumprimento de quaisquer das obrigações descritas nesta cláusula sujeitará A CONTRATADA a processo administrativo para apuração de responsabilidade e, consequente, sanção, sem prejuízo de outras penalidades.
- 23.16.** É dever da CONTRATADA orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.
- 23.17.** A CONTRATADA deverá exigir de subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.
- 23.18.** Quando aplicável, os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à ANPD, cabendo à CONTRATADA fornecer as informações e documentos que lhe forem solicitados para esse fim.
- 23.19.** A CONTRATANTE poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo a Contratada atender prontamente eventuais pedidos de comprovação formulados.
- 23.20.** Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.
- 23.20.1.** Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.
- 23.21** O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.
- 23.22** A CONTRATADA deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

24. OBRIGAÇÕES DA CONTRATANTE

- 24.1.** Fiscalizar o cumprimento do objeto e das demais cláusulas deste Termo de Referência e seus anexos;
- 24.2.** Proporcionar as condições necessárias para que a CONTRATADA possa cumprir o que estabelece este Termo de Referência e seus anexos;
- 24.3.** Designar pessoas para os papéis descritos quanto à fiscalização;
- 24.4.** Convocar, realizar e registrar reuniões junto à CONTRATADA;
- 24.5.** Verificar a execução dos serviços;
- 24.6.** Notificar formalmente a CONTRATADA, por escrito, acerca de defeitos, falhas, irregularidades ou imperfeições verificadas na execução dos serviços, fixando prazo razoável para sua correção, substituição ou reparação, total ou parcial, às suas expensas, quando cabível;
- 24.7.** Permitir a entrada dos funcionários da CONTRATADA, desde que devidamente identificados, garantindo que tenham acesso aos equipamentos e aos sistemas corporativos, bem como fornecer todos os meios necessários à execução dos serviços;
- 24.8.** Efetuar os pagamentos devidos à CONTRATADA no prazo e nas condições indicadas neste instrumento, desde que atenda as formalidades necessárias, e após aceitação dos serviços pelos meios convencionados;

- 24.9.** Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos profissionais da CONTRATADA ou o seu Preposto;
- 24.10.** Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da CONTRATADA, conforme determina a Lei, antes de efetuar o pagamento devido;
- 24.11.** Comunicar à CONTRATADA a necessidade de substituição de qualquer profissional que seja considerado inadequado para o exercício da função;
- 24.12.** Aplicar ao CONTRATADO as sanções previstas na lei e no Contrato.

25. OBRIGAÇÕES CONTRATUAIS ESPECÍFICAS REFERENTES AO LOTE 01

25.1. OBRIGAÇÕES DA CONTRATADA

- 25.1.1. Implantar, configurar e ativar as soluções de conectividade segura e de segurança da informação, conforme especificações técnicas estabelecidas no Termo de Referência, incluindo NGFW, SD-WAN, links e demais componentes previstos;
- 25.1.2 Fornecer todos os equipamentos, licenças, softwares, serviços e insumos necessários à plena execução do objeto, não sendo admitida cobrança adicional por itens essenciais à operação;
- 25.1.3 Garantir a interoperabilidade com o ambiente tecnológico existente da PRODEB, incluindo soluções de gerenciamento, autenticação, registro de logs e monitoramento, ou, alternativamente, fornecer solução equivalente ou superior às suas expensas;
- 25.1.4 Realizar a instalação, configuração, testes operacionais e ativação dos serviços nos prazos estabelecidos, incluindo realocação de pontos quando demandado;
- 25.1.5 Operar os serviços em regime contínuo, assegurando níveis de disponibilidade, desempenho e qualidade compatíveis com os Acordos de Nível de Serviço (SLA);
- 25.1.6 Executar serviços de suporte técnico, manutenção corretiva, preventiva e evolutiva, incluindo atualização de firmware, assinaturas e bases de segurança;
- 25.1.7 Realizar o monitoramento contínuo dos serviços e ativos implantados, com atuação proativa na identificação e comunicação de falhas, degradações e incidentes;
- 25.1.8 Atuar na resolução de incidentes dentro dos prazos estabelecidos em SLA, assegurando a completa restauração dos serviços;
- 25.1.9 Disponibilizar equipe técnica qualificada para atendimento remoto e presencial, conforme a criticidade do serviço e a localização das unidades;
- 25.1.10 Assegurar a segurança da informação, garantindo a confidencialidade, integridade e disponibilidade dos dados trafegados;
- 25.1.11 Manter registro e rastreabilidade das operações, eventos de segurança e atendimentos realizados, de forma a viabilizar auditoria, controle e fiscalização;
- 25.1.12 Cumprir integralmente as políticas, normas e diretrizes de segurança da informação e de TIC estabelecidas pelo Estado da Bahia, observando as orientações operacionais e os mecanismos de governança e monitoramento conduzidos pela PRODEB;
- 25.1.13 Não utilizar as instalações do contratante para fins alheios ao objeto contratual.

25.2. OBRIGAÇÕES DA SAEB

- 25.2.1 Atuar como gestora administrativa da Rede Governo;
- 25.2.2 Autorizar previamente a utilização da Ata de Registro de Preços pelos órgãos e entidades interessados, inclusive para fins de contratação, saque ou adesão, mediante análise de conformidade com o planejamento institucional e os limites legais;
- 25.2.3 Definir as diretrizes, políticas e orientações de natureza administrativa e de governança aplicáveis à execução do modelo da Rede Governo;

25.2.4 Analisar e aprovar previamente os instrumentos da fase preparatória da contratação, especialmente o Termo de Referência, o edital e seus anexos, quanto à aderência ao Estudo Técnico Preliminar, às diretrizes estabelecidas e às orientações jurídicas aplicáveis;

25.2.5 Acompanhar, em nível sistêmico, a execução da Rede Governo sob o aspecto administrativo, com foco na aderência ao modelo de governança, às diretrizes institucionais e à conformidade geral da contratação, sem prejuízo das atribuições de gestão e fiscalização contratual exercidas pelos órgãos contratantes;

25.2.6 Atuar de forma articuladora e orientativa junto à PRODEB e aos órgãos contratantes, apoiando a harmonização de entendimentos e a mitigação de questões administrativas que possam impactar o funcionamento global da Rede Governo;

25.2.7 Promover o alinhamento institucional entre os órgãos e entidades participantes da Rede Governo, assegurando a padronização, a coerência e a governança do modelo adotado.

25.3. OBRIGAÇÕES DA PRODEB

25.3.1 Atuar como responsável pela gestão técnica da Rede Governo, promovendo a coordenação operacional e tecnológica da solução;

25.3.2 Definir, manter e evoluir os padrões técnicos, arquiteturais e operacionais da solução, em conformidade com as diretrizes estabelecidas pela SAEB;

25.3.3 Validar tecnicamente as soluções implantadas pela CONTRATADA, assegurando sua aderência às especificações técnicas e aos padrões definidos;

25.3.4 Gerenciar e operar, direta ou indiretamente, a solução central de monitoramento, operação e gestão da Rede Governo;

25.3.5 Realizar o acompanhamento técnico da execução contratual, no que se refere ao desempenho, disponibilidade, capacidade e cumprimento dos níveis de serviço (SLA);

25.3.6 Implementar, operacionalizar e monitorar o cumprimento das políticas e diretrizes de segurança da informação e de conectividade definidas pelo Estado;

25.3.7 Integrar os serviços contratados ao ambiente central do Estado, incluindo datacenter, SOC e ferramentas corporativas de gestão;

25.3.8 Avaliar e manifestar-se tecnicamente quanto a implantações, alterações, expansões e mudanças de endereço, para fins de verificação de aderência aos padrões, à arquitetura e à operação da Rede Governo;

25.3.9 Consolidar, analisar e disponibilizar indicadores de desempenho e relatórios operacionais da solução;

25.3.10 Apoiar os órgãos contratantes na utilização dos serviços e na resolução de problemas de natureza técnica;

25.3.11 Assegurar a interoperabilidade entre as soluções implantadas e o ambiente tecnológico existente;

25.3.12 Coordenar, sob o ponto de vista técnico-operacional, a atuação da CONTRATADA em situações críticas e incidentes de maior impacto.

25.4. OBRIGAÇÕES DOS ÓRGÃOS CONTRANTES

25.4.1 Formalizar a contratação com base na Ata de Registro de Preços, observadas as condições nela estabelecidas e a legislação aplicável;

25.4.2 Emitir Ordens de Serviço contendo as informações necessárias à execução, incluindo endereços, contatos e demandas específicas para implantação e operação dos serviços;

25.4.3 Disponibilizar a infraestrutura mínima necessária à instalação e funcionamento dos equipamentos, incluindo energia elétrica, espaço físico adequado, acesso e demais requisitos técnicos;

25.4.4 Designar formalmente gestor e fiscal do contrato, responsáveis pelo acompanhamento e fiscalização da execução, nos termos da legislação aplicável;

25.4.5 Registrar solicitações, incidentes e demandas exclusivamente por meio dos canais oficiais definidos para a Rede Governo;

- 25.4.6 Acompanhar, fiscalizar e atestar a execução dos serviços em suas unidades, verificando a conformidade com as especificações contratuais e os níveis de serviço estabelecidos;
- 25.4.7 Comunicar tempestivamente à PRODEB e à CONTRATADA a ocorrência de falhas, indisponibilidades ou irregularidades na prestação dos serviços;
- 25.4.8 Zelar pelo uso adequado dos serviços e dos equipamentos disponibilizados, observando as condições contratuais e as orientações recebidas;
- 25.4.9 Cumprir as políticas, normas e diretrizes de segurança da informação e de uso da rede estabelecidas pelo Estado;
- 25.4.10 Efetuar os pagamentos devidos conforme as condições estabelecidas no contrato, quando aplicável.

26. ELEMENTOS NECESSÁRIOS À GESTÃO DO CONTRATO

- 26.1. No que se refere às contratações decorrentes da Ata de Registro de Preços, a designação do Gestor e do Fiscal do contrato caberá a cada órgão ou entidade contratante, mediante ato formal próprio, observado o regime jurídico aplicável e as normas internas de cada instituição, cabendo a esses agentes o acompanhamento, a fiscalização e a atestação da execução contratual, em conformidade com a legislação vigente e com as disposições constantes dos respectivos instrumentos contratuais.
- 26.2. Quanto às contratações realizadas pela PRODEB, a gestão e a fiscalização dos contratos decorrentes da Ata de Registro de Preços observarão as disposições do Capítulo V, Seção III, do RLC/PRODEB, especialmente o disposto nos arts. 184 a 191.
- 26.2.1. As atribuições do Gestor e do Fiscal do contrato, no âmbito da PRODEB, serão exercidas nos termos do disposto no art. 186 e nos arts. 187 a 190, respectivamente, do RLC da PRODEB.
- 26.2.2. O Gestor e o Fiscal do contrato serão formalmente designados no momento da contratação, mediante ato administrativo próprio, em conformidade com as normas internas da Companhia.

VI. INFORMAÇÕES ADICIONAIS

27. FORMA DE COMUNICAÇÃO

- 27.1. A tramitação de documentos entre CONTRATANTE e a CONTRATADA deverá ser rigorosamente controlada através de documentos protocolados fisicamente ou enviados através de meio eletrônico.

28. EXIGÊNCIA DE PROGRAMA DE INTEGRIDADE PARA O LOTE 01

- 28.1. Considerando tratar-se de contratação de grande vulto, nos termos do art. 6º, inciso XXII, da Lei Federal nº 14.133/2021, e o disposto no art. 25, §4º, da mesma Lei, a CONTRATADA deverá comprovar a implantação de Programa de Integridade no prazo de 06 (seis) meses, contado da celebração do contrato.
- 28.2 A comprovação da implantação deverá ocorrer mediante apresentação de documentação idônea, nos termos definidos no referido Decreto Estadual nº 23.356/2025, e o Programa deverá permanecer ativo e em funcionamento durante toda a vigência contratual.
- 28.3 O acompanhamento da implantação e da manutenção do Programa de Integridade será realizado pela CONTRATANTE, conforme os mecanismos de monitoramento previstos no Decreto Estadual nº 23.356/2025, e o eventual descumprimento da obrigação sujeitará a CONTRATADA às consequências administrativas previstas na legislação aplicável, sem prejuízo das demais sanções cabíveis.

29. REQUISITOS DE SUSTENTABILIDADE E ACESSIBILIDADE

LOTE 01

A solução de conectividade segura deverá ser concebida, implantada e operada em consonância com princípios de sustentabilidade ambiental, eficiência no uso de recursos e responsabilidade socioambiental, bem como com diretrizes de acessibilidade aplicáveis aos serviços públicos digitais, de modo a assegurar aderência às políticas públicas vigentes e ao interesse público.

No que se refere à sustentabilidade, a solução deverá priorizar modelos de prestação baseados em uso eficiente e racional de recursos tecnológicos, privilegiando arquiteturas que reduzam a necessidade de aquisição, transporte, substituição frequente e descarte de equipamentos físicos, em consonância com o modelo de prestação de solução como serviço. A utilização de infraestrutura compartilhada, virtualizada ou gerenciada, quando aplicável, deverá contribuir para a redução do consumo energético, da geração de resíduos e da pegada ambiental associada à operação da Rede Governo.

Os requisitos de sustentabilidade e acessibilidade deverão ser incorporados de forma transversal à solução, sem comprometer os requisitos técnicos, de segurança da informação, de desempenho e de continuidade operacional da Rede Governo.

LOTE 02

A implementação deverá observar critérios de sustentabilidade tecnológica e ambiental sempre que aplicáveis, priorizando eficiência de recursos e práticas que reduzam impacto ambiental.

As interfaces usuais deverão observar diretrizes de acessibilidade digital compatíveis com padrões governamentais, assegurando usabilidade por parte dos servidores e, quando aplicável, cidadãos com deficiência.

30. SANÇÕES ADMINISTRATIVAS

30.1. Serão aplicadas sanções administrativas ao Licitante que cometer qualquer prática considerada ilícita conforme exposto no Art. 212 a 226 do Regulamento de Licitações e Contratos da PRODEB, podendo incidir, em caso de descumprimento contratual, multas ou descontos, bem como, em casos mais graves, rescisão do mesmo, observadas, conforme o ente contratante e o regime jurídico aplicável, as disposições da Lei Federal nº 14.133/2021, da Lei Estadual nº 14.634/2023 e do Decreto Estadual nº 23.113/2024, no que couber.

30.2. No caso de descumprimento total da obrigação principal, será aplicada multa compensatória no percentual de 15% (quinze por cento) incidente sobre o valor global do contrato.

30.3. Caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicada multa compensatória no percentual de 15% (quinze por cento) incidente sobre o saldo do contrato, isto é, sobre a diferença entre o valor global do contrato e o valor da parte do serviço já realizado.

30.4. No caso de descumprimento da obrigação acessória, será aplicada multa compensatória no percentual de 15% (quinze por cento) incidente sobre o valor da obrigação descumprida ou da estimativa arbitrada do seu custo.

30.5. No caso de recusa injustificada do adjudicatário em assinar o termo de contrato, em aceitar ou retirar o instrumento equivalente, ou, quando for o caso, em assinar a ata de registro de preços, ou praticar condutas a elas equiparadas, será aplicada multa compensatória no percentual de 15% (quinze por cento) incidente sobre o valor correspondente ao objeto adjudicado ou, quando for o caso, da estimativa da contratação.

30.6. O atraso injustificado na execução do Contrato ensejará a aplicação de multa moratória no percentual de 0,1% (um décimo por cento) ao dia, incidente sobre o valor da obrigação descumprida ou da estimativa arbitrada do seu custo, observado o percentual máximo total de 30% (trinta por cento).

- 30.7.** O atraso injustificado do prazo fixado para apresentação, suplementação ou reposição de garantia contratual ensejará a aplicação de multa moratória no percentual de 0,1% (um décimo por cento) ao dia, incidente sobre o valor global do contrato.
- 30.8.** A aplicação de multa de mora não impedirá que a CONTRATANTE a converta em compensatória e promova a extinção unilateral do Contrato com a aplicação cumulada de outras sanções previstas no instrumento contratual e na legislação vigente.
- 30.9.** Na hipótese do subitem anterior, se o cálculo da multa moratória atingir o patamar correspondente ao valor máximo da multa compensatória, o recebimento do objeto deverá ser recusado, salvo justificativa escrita devidamente fundamentada, sem prejuízo da aplicação das demais sanções previstas no instrumento contratual e na legislação vigente.
- 30.10.** A aplicação das sanções administrativas previstas neste item observará, conforme o ente contratante e o regime jurídico aplicável, as disposições da legislação federal e estadual vigente sobre infrações e sanções administrativas, inclusive quanto à classificação das infrações, critérios de dosimetria e à possibilidade de adoção de mecanismos de solução consensual, como a transação administrativa.

31. TERMO DE COMPROMISSO E DE CONFIDENCIALIDADE

- 31.1.** A CONTRATADA compromete-se a cumprir e obedecer à **Política de Segurança da Informação do Governo do Estado da Bahia**, disponibilizada através do link: <https://www.ba.gov.br/administracao/node/154>
- 31.2.** A CONTRATADA deverá assim ar **Termo de Compromisso, Sigilo e Confidencialidade**, constante em **Anexo** deste Termo, no momento da assinatura do contrato.

32. GARANTIA CONTRATUAL

- 32.1.** No que se refere à garantia contratual, deverá ser exigida a prestação de garantia correspondente a 5% (cinco por cento) do valor do contrato, em conformidade com o art. 98 da Lei Federal nº 14.133/2021, aplicada no âmbito do Estado da Bahia por força da Lei Estadual nº 14.634/2023. A fixação desse percentual mostra-se proporcional ao risco envolvido, à natureza continuada da contratação e à criticidade da solução, atendendo às diretrizes legais aplicáveis.
- 32.2.** A exigência de garantia contratual é compatível, ainda, com o regime procedimental adotado pela PRODEB, na condição de entidade delegada para a condução do certame, encontrando respaldo no art. 158, §2º, do Regulamento de Licitações e Contratos da PRODEB, que admite a exigência de garantia nos limites estabelecidos pela legislação vigente.
- 32.3.** A garantia contratual deverá assegurar a cobertura de obrigações relacionadas à implantação da solução, à operação assistida, à manutenção, aos serviços de suporte técnico e garantia, ao cumprimento dos níveis de serviço pactuados e à correção de falhas, defeitos ou inconformidades identificadas durante a execução contratual, sem prejuízo da continuidade dos serviços públicos essenciais.
- 32.4** A garantia, qualquer que seja a modalidade eleita, deverá assegurar o pagamento de:
- a) prejuízos advindos do não cumprimento do objeto do contrato;
 - b) prejuízos diretos causados à PRODEB decorrentes de culpa ou dolo durante a execução do contrato;
 - c) multas moratórias e compensatórias aplicadas pela PRODEB ao contratado; e
 - d) obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pelo contratado, quando couber.

33. MATRIZ DE RISCOS

- 33.1.** Este Termo de Referência foi elaborado com base nos dados levantados e explicitados no documento denominado MATRIZ DE RISCOS, em anexo.

Salvador, 24 de abril de 2026.

Elmo Sales dos Santos

Assessor Especial

De acordo,

Carlos Augusto Borges Silva

Diretor de Infraestrutura Tecnológica e Conectividade

ANEXO I

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Os abaixo-assinados, de um lado a Cia. de Processamento de dados do Estado da Bahia - PRODEB, CNPJ nº 13.579.586/001-32, situada na cidade de Salvador, à Av. 4, nº 410, Centro Administrativo da Bahia – CAB, SalvadorBahia, doravante denominada CONTRATANTE, e de outro lado _____, CNPJ nº _____/_____, situada na cidade de _____, à Rua: _____, bairro _____, doravante denominada CONTRATADA, têm entre si justa e acertada, a celebração do presente TERMO DE SIGILO E CONFIDENCIALIDADE, através do qual a CONTRATADA aceita não divulgar sem autorização prévia e formal segredos e informações sensíveis de propriedade da PRODEB e de seus clientes e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

PRIMEIRA – A CONTRATADA reconhece que em razão das suas atividades profissionais, estabelece contato com informações sigilosas, que devem ser entendidas como segredo. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios Colaboradores da CONTRATADA, sem a expressa e escrita autorização da CONTRATANTE.

SEGUNDA - As informações a serem tratadas confidencialmente são aquelas assim consideradas no âmbito da PRODEB, transmitidas por meios escritos, eletrônicos, verbais ou quaisquer outros, e que, por sua natureza, não são ou não deveriam ser de conhecimento de terceiros, tais como:

1. Toda informação relacionada a computador e componentes de software em geral, programas existentes (código fonte/código objeto), ou em fase de desenvolvimento no âmbito da empresa, inclusive fluxogramas, listagens, documentação, estatísticas, especificações, avaliações, resultado de testes, arquivo de dados e versões “beta” de quaisquer programas e rotinas;
2. Documentos, informações e dados armazenados de atuação consultiva e contenciosa, de estratégias ou demais dados e/ou informações de caráter sigiloso ou restrito;
3. Informações e documentos relativos às estratégias de marketing, de negócios, de clientes e os seus respectivos dados, pesquisas de mercado, armazenados sob qualquer forma;
4. Informações de projetos, metodologias, ferramentas de desenvolvimento de aplicativos e serviços desenvolvidos pela PRODEB;
5. Números e valores financeiros da empresa tais como: inadimplência, relação de salários, fluxo de caixa, informações de custos, dentre outros;
6. Informações referentes a dados pessoais e/ou dados pessoais sensíveis.

TERCEIRA – A CONTRATADA reconhece que a lista acima é meramente exemplificativa e ilustrativa e que outras hipóteses de confidencialidade que já existam ou que venham a surgir no futuro devem ser mantidas sob segredo. Em caso de dúvida acerca da confidencialidade de determinada informação a CONTRATADA deve tratar a mesma sob sigilo até que seja autorizado, formalmente, a tratá-la de forma diferente pela CONTRATANTE. Em hipótese alguma a CONTRATADA deve interpretar o silêncio da Empresa como liberação de quaisquer dos compromissos ora assumidos.

QUARTA - A CONTRATADA está ciente de que o serviço de correio eletrônico corporativo, caso seja fornecido pela CONTRATANTE para o exercício das atividades, é exclusivo para assuntos pertinentes ao objeto do contrato e reconhece que a CONTRATANTE tem pleno acesso à essas contas corporativas para quaisquer fins, tais como: auditoria, encaminhamento de assuntos pendentes, configuração de resposta automática, redirecionamento e recuperação de e-mails.

QUINTA – A CONTRATADA reconhece que, ao término do presente contrato _____, deverá entregar à CONTRATANTE todo e qualquer material de propriedade desta, inclusive notas pessoais envolvendo matérias sigilosas relacionadas com a _____, registros de documentos de qualquer natureza que tenham sido usados, criados ou estado sob seu controle. A CONTRATADA também assume o compromisso de não utilizar qualquer informação adquirida quando de suas atividades para a CONTRATANTE.

SEXTA – A CONTRATADA deve assegurar que todos os seus colaboradores guardarão sigilo sobre as informações que porventura tiverem acesso, e que os mesmos se comprometem a informar imediatamente ao seu superior hierárquico,

qualquer violação das regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional.

Parágrafo Primeiro: A apresentação dos Termos de Sigilo e Confidencialidade de seus colaboradores não exime a CONTRATADA das penalidades por violação das regras por parte destes.

Parágrafo segundo: A CONTRATADA deverá fornecer cópia de todos os termos firmados com seus colaboradores à CONTRATANTE no prazo de 10 (dez) dias após assinatura dos respectivos termos.

Parágrafo Terceiro: Sempre que um colaborador for admitido, A CONTRATADA deverá fornecer cópia dos novos termos firmados no prazo de 2 (dois) dias após assinatura dos respectivos termos.

SÉTIMA - O atendimento deste Termo de Sigilo e Confidencialidade bem como da das Diretrizes Básicas da Política de Segurança da Informação devem ser incorporados formalmente ao contrato de trabalho dos funcionários da CONTRATADA que prestarem serviços à CONTRATANTE.

OITAVA – A CONTRATADA deverá atender às diretrizes estabelecidas na Política de Segurança da Informação definida pela CONTRATANTE.

NONA - A CONTRATADA declara, por fim, que as obrigações a que alude este Termo perdurarão após o término do contrato AA/NNNN-00, e abrangem, além das informações de que venha a tomar conhecimento, aquelas que já possui na presente data.

DÉCIMA - O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização civil e criminal, de acordo com a legislação vigente.

Em, ____ de _____ de 20 ____.

Responsável pelo Contrato – CONTRATANTE

Responsável pelo Contrato - CONTRATADA

ANEXO II - MODELO DE PROPOSTA

LOTE 01

Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor mensal unitário (R\$) A	Valor unitário para 60 meses (R\$) B = A * 60	Valor Total 60 meses (R\$) C = B * QTD
1	02.81.00.00192352-8	Solução de Conectividade Segura TIPO 01 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 500MB.	Unidade	1589			
2	02.81.00.00192353-6	Solução de Conectividade Segura TIPO 02 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 2 links (redundância) de internet banda larga com velocidade de 500MB.	Unidade	707			
3	02.81.00.00192354-4	Solução de Conectividade Segura TIPO 03 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN e 1 link de internet banda larga com velocidade de 1GB.	Unidade	109			

4	02.81.00.00192355-2	Solução de Conectividade Segura TIPO 04 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 2 links (redundância) de internet banda larga com velocidade de 1GB.	Unidade	167			
5	02.81.00.00192356-0	Solução de Conectividade Segura TIPO 05 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários em unidades remotas que não possuem viabilidade de conexão via fibra ótica, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 1 link satélite com velocidade de 100 MB.	Unidade	149			
6	02.81.00.00192357-9	Solução de Conectividade Segura TIPO 06 Solução de conectividade segura para unidades críticas prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender até 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN e 1 link de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.	Unidade	101			

7	02.81.00.00192358-7	Solução de Conectividade Segura TIPO 07 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 500MB.	Unidade	54			
8	02.81.00.00192359-5	Solução de Conectividade Segura TIPO 08 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 500MB.	Unidade	16			
9	02.81.00.00192360-9	Solução de Conectividade Segura TIPO 09 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link de internet banda larga com velocidade de 1GB.	Unidade	78			

10	02.81.00.00192361-7	Solução de Conectividade Segura TIPO 10 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 2 links de internet banda larga com velocidade de 1GB.	Unidade	33			
11	02.81.00.00192362-5	Solução de Conectividade Segura TIPO 11 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB.	Unidade	91			
12	02.81.00.00192363-3	Solução de Conectividade Segura TIPO 12 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para atender unidades que já possuem firewall de próxima geração (NGFW) com tecnologia SDWAN ou para atender unidades que necessitam ampliar a velocidade de conexão contemplando 1 link satélite com velocidade de 100 MB e 1 link de internet banda larga com velocidade de 500MB.	Unidade	14			

13	02.81.00.00192364-1	Solução de Conectividade Segura TIPO 13 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades com até 40 usuários e que já possuem link de internet contemplando 01 firewall de próxima geração (NGFW) com tecnologia SD-WAN.	Unidade	105			
14	02.81.00.00192365-0	Solução de Conectividade Segura TIPO 14 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, com capacidade para atender unidades acima de 40 usuários e que já possuem link de internet contemplando 01 firewall de próxima geração (NGFW) com tecnologia SD-WAN.	Unidade	50			
15	02.81.00.00192366-8	Solução de Conectividade Segura TIPO 15 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN, 2 links (redundância) de internet banda larga com velocidade de 500MB e 1 link satélite com velocidade de 100 MB.	Unidade	20			

16	02.81.00.00192367-6	Solução de Conectividade Segura TIPO 16 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, para unidades críticas com capacidade para atender acima de 40 usuários, incluso proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SDWAN, 2 links (redundância) de internet banda larga com velocidade de 1GB e 1 link satélite com velocidade de 100 MB.	Unidade	16			
17	02.81.00.00192368-4	Solução de Conectividade Segura TIPO 17 Solução de conectividade segura prestada em regime contínuo e remunerada por valor mensal, destinada a unidades com até 05 usuários, contemplando 1 link de internet banda larga com velocidade de 200 Mbps e mecanismos de segurança providos de forma centralizada, sob gestão da PRODEB, sem a necessidade de firewall de borda dedicado na unidade.	Unidade	369			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)	
18	02.81.00.00192370-6	Serviço de Mudança de Endereço – até 300 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	137			

19	02.81.00.00192371-4	Serviço de Mudança de Endereço – acima de 300 km até 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	144			
20	02.81.00.00192372-2	Serviço de Mudança de Endereço – acima de 600 km de Salvador/BA Serviço eventual de mudança de endereço de ponto de acesso com solução de conectividade segura ativa, contemplando a realocação da infraestrutura, reconfiguração dos equipamentos e testes operacionais necessários à continuidade do serviço.	Unidade	108			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor mensal unitário (R\$) A	Valor unitário para 60 meses (R\$) B = A * 60	Valor Total 60 meses (R\$) C = B * QTD
21	02.81.09.00008168-0	Solução de Operação e Monitoramento Central, prestada em regime contínuo e remunerada por valor mensal, dimensionada para atender até 500 (quinhentas) unidades de solução de conectividade segura em operação	Unidade	10			
22	02.81.09.00008169-8	Solução de Monitoramento e Relatoria De Logs Tipo I	Unidade	02			
23	02.81.00.00192944-5	Solução de Monitoramento e Relatoria De Logs Tipo II	Unidade	50			

24	02.81.00.00192945-3	Solução de Monitoramento e Relatoria De Logs Tipo III	Unidade	04			
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)	
25	02.81.00.00192946-1	UST – Unidade de Serviços Técnicos	Unidade	5.000			
Valor Global do Lote 01:							

LOTE 02

Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)
1	02.81.00.00192373-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600E, pelo período de 12 meses	Unidade	04		
2	02.81.00.00192374-9	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 601E, pelo período de 12 meses	Unidade	04		
3	02.81.00.00192375-7	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 400F, pelo período de 12 meses	Unidade	08		
4	02.81.00.00192376-5	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200F, pelo período de 12 meses	Unidade	09		
5	02.81.00.00192377-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200E, pelo período de 12 meses	Unidade	04		
6	02.81.00.00192378-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 100F, pelo período de 12 meses	Unidade	24		

7	02.81.00.00192379-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 80F, pelo período de 12 meses	Unidade	12		
8	02.81.00.00192380-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 60F, pelo período de 12 meses	Unidade	300		
9	02.81.00.00192381-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 61F, pelo período de 12 meses	Unidade	300		
10	02.81.00.00192382-0	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 150G, pelo período de 12 meses	Unidade	04		
11	02.81.00.00192383-8	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 300G, pelo período de 12 meses	Unidade	04		
12	02.81.00.00192384-6	Serviço de Licenciamento e Atualização das Funcionalidades de Autenticação Centralizada de Usuários Marca Fortinet Modelo FortiAuthenticator 800F, pelo período de 12 meses	Unidade	04		
13	02.81.00.00192385-4	Solução De Segurança de Rede NGFW TIPO I, com licenciamento pelo período de 12 meses	Unidade	04		
14	02.81.00.00192386-2	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede - Segmentação Interna TIPO I, pelo período de 12 meses	Unidade	04		

15	02.81.00.00192947-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3700F, pelo período de 12 meses	Unidade	04		
16	02.81.00.00192948-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3301E, pelo período de 12 meses	Unidade	04		
17	02.81.00.00192949-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3000D, pelo período de 12 meses	Unidade	02		
18	02.81.00.00192950-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600F, pelo período de 12 meses	Unidade	04		
19	02.81.00.00192951-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 40F, pelo período de 12 meses	Unidade	60		
20	02.81.00.00192952-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate-VM08, pelo período de 12 meses	Unidade	02		
21	02.81.00.00192953-4	Serviço de Licenciamento e Atualização das Funcionalidades de WAF Marca Fortinet Modelo FortiWeb2000F, pelo período de 12 meses	Unidade	04		
22	02.81.00.00192954-2	Serviço de Licenciamento e Atualização das Funcionalidades de ADC Marca Fortinet Modelo FortiADC-400F, pelo período de 12 meses	Unidade	02		

23	02.80.00.00192955-0	Serviço de Licenciamento e Atualização das Funcionalidades de Gerenciador Centralizada de Dispositivos Marca Fortinet Modelo FortiManager 3000G, pelo período de 12 meses	Unidade	02		
24	02.81.00.00192956-9	Serviço de Licenciamento e Atualização das Funcionalidades de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	02		
25	02.81.00.00192957-7	Serviço de Upgrade para 50 Devices e 500 EPS de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	04		
26	02.81.00.00192958-5	Solução De Segurança de Aplicações WAF - TIPO I, com licenciamento pelo período de 12 meses	Unidade	02		
27	02.81.00.00192959-3	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF - TIPO I, pelo período de 12 meses	Unidade	02		
28	02.81.00.00192989-5	Solução De Segurança de Aplicações WAF - TIPO II, com licenciamento pelo período de 12 meses	Unidade	10		
29	02.81.00.00192990-9	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF –TIPO II, pelo período de 12 meses	Unidade	10		
30	02.81.00.00192962-3	Solução de Segurança de Aplicações WAF para Ambientes Híbridos, com licenciamento pelo período de 12 meses	Unidade	10		
31	02.81.00.00192963-1	Serviço de Licenciamento e Atualização das Funcionalidades de Solução de Segurança de Aplicações WAF para Ambientes Híbridos, pelo período de 12 meses	Unidade	10		

32	02.81.00.00192964-0	Solução de Segurança Decoy/Honeypot, com licenciamento pelo período de 12 meses	Unidade	06		
33	02.81.00.00192965-8	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança Decoy/Honeypot, pelo período de 12 meses	Unidade	06		
34	02.81.00.00192966-6	Solução de Segurança de Rede NGFW TIPO II, com licenciamento pelo período de 12 meses	Unidade	100		
35	02.81.00.00192967-4	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna TIPO II, pelo período de 12 meses	Unidade	100		
36	02.81.00.00192968-2	Solução de Segurança de Rede NGFW TIPO III, com licenciamento pelo período de 12 meses	Unidade	50		
37	02.81.00.00192969-0	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna TIPO III, pelo período de 12 meses	Unidade	50		
Valor Global do Lote 02						R\$

Declaramos que temos conhecimento e concordamos com todos os itens mencionados no Termo de Referência, documento base para a presente proposta de preços.

Nos preços contratados estão incluídos todos os custos com material de consumo, salários, encargos sociais, previdenciários e trabalhistas de todo o pessoal da CONTRATADA, como também fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, tributos, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela CONTRATADA das obrigações.

RAZÃO SOCIAL	CNPJ
TELEFONE	PRAZO DE ENTREGA
DATA	VALIDADE DA PROPOSTA
RESPONSÁVEL/CPF	ENDEREÇO

ANEXO III – ORÇAMENTO ESTIMADO EM PLANILHAS

LOTE 1 - VALOR REFERENCIAL							
Item	Código SIMPAS	Descrição Resumida	Unidade	QTD	Valor mensal unitário (A)	Valor unitário para 60 meses (B = A*60)	Valor Total 60 meses (C = B*QTD)
1	02.81.00.00192352-8	Solução de Conectividade Segura TIPO 01	Unidade	1589	R\$ 1.609,00	R\$ 96.540,00	R\$ 153.402.060,00
2	02.81.00.00192353-6	Solução de Conectividade Segura TIPO 02	Unidade	707	R\$ 2.455,00	R\$ 147.300,00	R\$ 104.141.100,00
3	02.81.00.00192354-4	Solução de Conectividade Segura TIPO 03	Unidade	109	R\$ 4.648,00	R\$ 278.880,00	R\$ 30.397.920,00
4	02.81.00.00192355-2	Solução de Conectividade Segura TIPO 04	Unidade	167	R\$ 6.339,00	R\$ 380.340,00	R\$ 63.516.780,00
5	02.81.00.00192356-0	Solução de Conectividade Segura TIPO 05	Unidade	149	R\$ 2.845,00	R\$ 170.700,00	R\$ 25.434.300,00
6	02.81.00.00192357-9	Solução de Conectividade Segura TIPO 06	Unidade	101	R\$ 3.691,00	R\$ 221.460,00	R\$ 22.367.460,00
7	02.81.00.00192358-7	Solução de Conectividade Segura TIPO 07	Unidade	54	R\$ 846,00	R\$ 50.760,00	R\$ 2.741.040,00
8	02.81.00.00192359-5	Solução de Conectividade Segura TIPO 08	Unidade	16	R\$ 1.692,00	R\$ 101.520,00	R\$ 1.624.320,00
9	02.81.00.00192360-9	Solução de Conectividade Segura TIPO 09	Unidade	78	R\$ 1.692,00	R\$ 101.520,00	R\$ 7.918.560,00
10	02.81.00.00192361-7	Solução de Conectividade Segura TIPO 10	Unidade	33	R\$ 3.383,00	R\$ 202.980,00	R\$ 6.698.340,00
11	02.81.00.00192362-5	Solução de Conectividade Segura TIPO 11	Unidade	91	R\$ 2.082,00	R\$ 124.920,00	R\$ 11.367.720,00
12	02.81.00.00192363-3	Solução de Conectividade Segura TIPO 12	Unidade	14	R\$ 2.928,00	R\$ 175.680,00	R\$ 2.459.520,00
13	02.81.00.00192364-1	Solução de Conectividade Segura TIPO 13	Unidade	105	R\$ 763,00	R\$ 45.780,00	R\$ 4.806.900,00
14	02.81.00.00192365-0	Solução de Conectividade Segura TIPO 14	Unidade	50	R\$ 2.957,00	R\$ 177.420,00	R\$ 8.871.000,00
15	02.81.00.00192366-8	Solução de Conectividade Segura TIPO 15	Unidade	20	R\$ 6.730,00	R\$ 403.800,00	R\$ 8.076.000,00
16	02.81.00.00192367-6	Solução de Conectividade Segura TIPO 16	Unidade	16	R\$ 8.421,00	R\$ 505.260,00	R\$ 8.084.160,00
17	02.81.00.00192368-4	Solução de Conectividade Segura TIPO 17	Unidade	369	R\$ 781,00	R\$ 46.860,00	R\$ 17.291.340,00
Item	Código SIMPAS	Descrição Resumida	Unidade	QTD	Valor unitário		Valor Total
18	02.81.00.00192370-6	Serviço de Mudança de Endereço – até 300 km de Salvador/BA.	Unidade	137	R\$ 1.105,00		R\$ 151.385,00
19	02.81.00.00192371-4	Serviço de Mudança de Endereço – acima de 300 km até 600 km de Salvador/BA.	Unidade	144	R\$ 1.486,00		R\$ 213.984,00
20	02.81.00.00192372-2	Serviço de Mudança de Endereço – acima de 600 km de Salvador/BA.	Unidade	108	R\$ 1.772,00		R\$ 191.376,00
Item	Código SIMPAS	Descrição Resumida	Unidade	QTD	Valor mensal unitário (A)	Valor unitário para 60 meses (B = A*60)	Valor Total 60 meses (C = B*QTD)
21	02.81.09.00008168-0	Solução de Operação e Monitoramento Central	Unidade	10	R\$ 146.450,00	R\$ 8.787.000,00	R\$ 87.870.000,00
22	02.81.09.00008169-8	Solução de Monitoramento e Relatoria De Logs Tipo I	Unidade	2	R\$ 51.358,00	R\$ 3.081.480,00	R\$ 6.162.960,00
23	02.81.00.00192944-5	Solução de Monitoramento e Relatoria De Logs Tipo II	Unidade	50	R\$ 1.400,00	R\$ 84.000,00	R\$ 4.200.000,00
24	02.81.00.00192945-3	Solução de Monitoramento e Relatoria De Logs Tipo III	Unidade	4	R\$ 20.544,00	R\$ 1.232.640,00	R\$ 4.930.560,00
Item	Código SIMPAS	Descrição Resumida	Unidade	QTD	Valor unitário		Valor Total
25	02.81.00.00192946-1	UST – Unidade de Serviços Técnicos	Unidade	5000	R\$ 1.413,00		R\$ 7.065.000,00
Valor Global Referencial do Lote 01							R\$ 589.983.785,00

LOTE 02 - VALOR REFERENCIAL						
Item	Código SIMPAS	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário (R\$)	Valor Total (R\$)
1	02.81.00.00192373-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600E, pelo período de 12 meses	Unidade	4	R\$ 85.732,00	R\$ 342.928,00
2	02.81.00.00192374-9	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 601E, pelo período de 12 meses	Unidade	4	R\$ 96.181,00	R\$ 384.724,00
3	02.81.00.00192375-7	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 400F, pelo período de 12 meses	Unidade	8	R\$ 79.696,00	R\$ 637.568,00
4	02.81.00.00192376-5	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200F, pelo período de 12 meses	Unidade	9	R\$ 34.856,00	R\$ 313.704,00
5	02.81.00.00192377-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 200E, pelo período de 12 meses	Unidade	4	R\$ 18.164,00	R\$ 72.656,00
6	02.81.00.00192378-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 100F, pelo período de 12 meses	Unidade	24	R\$ 16.976,00	R\$ 407.424,00
7	02.81.00.00192379-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 80F, pelo período de 12 meses	Unidade	12	R\$ 9.620,00	R\$ 115.440,00
8	02.81.00.00192380-3	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 60F, pelo período de 12 meses	Unidade	300	R\$ 4.370,00	R\$ 1.311.000,00
9	02.81.00.00192381-1	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 61F, pelo período de 12 meses	Unidade	300	R\$ 5.627,00	R\$ 1.688.100,00
10	02.81.00.00192382-0	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 150G, pelo período de 12 meses	Unidade	4	R\$ 9.728,00	R\$ 38.912,00
11	02.81.00.00192383-8	Serviço de Licenciamento e Atualização das Funcionalidades de Repositório e Relatoria de Logs Marca Fortinet Modelo FortiAnalyzer 300G, pelo período de 12 meses	Unidade	4	R\$ 21.885,00	R\$ 87.540,00
12	02.81.00.00192384-6	Serviço de Licenciamento e Atualização das Funcionalidades de Autenticação Centralizada de Usuários Marca Fortinet Modelo FortiAuthenticator 800F, pelo período de 12 meses	Unidade	4	R\$ 43.247,00	R\$ 172.988,00
13	02.81.00.00192385-4	Solução De Segurança de Rede NGFW TIPO I, com licenciamento pelo período de 12 meses	Unidade	4	R\$ 413.696,00	R\$ 1.654.784,00
14	02.81.00.00192386-2	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede - Segmentação Interna TIPO I, pelo período de 12 meses	Unidade	4	R\$ 144.856,00	R\$ 579.424,00
15	02.81.00.00192947-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3700F, pelo período de 12 meses	Unidade	4	R\$ 1.445.724,00	R\$ 5.782.896,00
16	02.81.00.00192948-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3301E, pelo período de 12 meses	Unidade	4	R\$ 272.233,00	R\$ 1.088.932,00
17	02.81.00.00192949-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 3000D, pelo período de 12 meses	Unidade	2	R\$ 366.634,00	R\$ 733.268,00
18	02.81.00.00192950-0	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 600F, pelo período de 12 meses	Unidade	4	R\$ 115.828,00	R\$ 463.312,00
19	02.81.00.00192951-8	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate 40F, pelo período de 12 meses	Unidade	60	R\$ 3.113,00	R\$ 186.780,00
20	02.81.00.00192952-6	Serviço de Licenciamento e Atualização das Funcionalidades de NGFW Marca Fortinet Modelo FortiGate-VM08, pelo período de 12 meses	Unidade	2	R\$ 203.326,00	R\$ 406.652,00
21	02.81.00.00192953-4	Serviço de Licenciamento e Atualização das Funcionalidades de WAF Marca Fortinet Modelo FortiWeb2000F, pelo período de 12 meses	Unidade	4	R\$ 543.208,00	R\$ 2.172.832,00
22	02.81.00.00192954-2	Serviço de Licenciamento e Atualização das Funcionalidades de ADC Marca Fortinet Modelo FortiADC-400F, pelo período de 12 meses	Unidade	2	R\$ 170.199,00	R\$ 340.398,00
23	02.80.00.00192955-0	Serviço de Licenciamento e Atualização das Funcionalidades de Gerenciador Centralizada de Dispositivos Marca Fortinet Modelo FortiManager 3000G, pelo período de 12 meses	Unidade	2	R\$ 335.535,00	R\$ 671.070,00
24	02.81.00.00192956-9	Serviço de Licenciamento e Atualização das Funcionalidades de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	2	R\$ 922.138,00	R\$ 1.844.276,00
25	02.81.00.00192957-7	Serviço de Upgrade para 50 Devices e 500 EPS de SIEM Marca Fortinet Modelo FortiSiem VM, pelo período de 12 meses	Unidade	4	R\$ 171.200,00	R\$ 684.800,00
26	02.81.00.00192958-5	Solução De Segurança de Aplicações WAF - TIPO I, com licenciamento pelo período de 12 meses	Unidade	2	R\$ 1.279.350,00	R\$ 2.558.700,00
27	02.81.00.00192959-3	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF - TIPO I, pelo período de 12 meses	Unidade	2	R\$ 608.393,00	R\$ 1.216.786,00
28	02.81.00.00192989-5	Solução De Segurança de Aplicações WAF - TIPO II, com licenciamento pelo período de 12 meses	Unidade	10	R\$ 260.921,00	R\$ 2.609.210,00
29	02.81.00.00192990-9	Serviço de Licenciamento e Atualização das Funcionalidades de Web Application Firewall para o WAF –TIPO II, pelo período de 12 meses	Unidade	10	R\$ 119.157,00	R\$ 1.191.570,00
30	02.81.00.00192962-3	Solução de Segurança de Aplicações WAF para Ambientes Híbridos, com licenciamento pelo período de 12 meses	Unidade	10	R\$ 69.591,00	R\$ 695.910,00
31	02.81.00.00192963-1	Serviço de Licenciamento e Atualização das Funcionalidades de Solução de Segurança de Aplicações WAF para Ambientes Híbridos, pelo período de 12 meses	Unidade	10	R\$ 65.652,00	R\$ 656.520,00
32	02.81.00.00192964-0	Solução de Segurança Decoy/Honeypot, com licenciamento pelo período de 12 meses	Unidade	6	R\$ 128.556,00	R\$ 771.336,00
33	02.81.00.00192965-8	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança Decoy/Honeypot, pelo período de 12 meses	Unidade	6	R\$ 50.010,00	R\$ 300.060,00
34	02.81.00.00192966-6	Solução de Segurança de Rede NGFW TIPO II, com licenciamento pelo período de 12 meses	Unidade	100	R\$ 15.264,00	R\$ 1.526.400,00
35	02.81.00.00192967-4	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna TIPO II, pelo período de 12 meses	Unidade	100	R\$ 5.090,00	R\$ 509.000,00
36	02.81.00.00192968-2	Solução de Segurança de Rede NGFW TIPO III, com licenciamento pelo período de 12 meses	Unidade	50	R\$ 47.063,00	R\$ 2.353.150,00
37	02.81.00.00192969-0	Serviço de Licenciamento e Atualização das Funcionalidades de Segurança de Rede – Segmentação Interna TIPO III, pelo período de 12 meses	Unidade	50	R\$ 16.814,00	R\$ 840.700,00
Valor Global do Lote 02						R\$ 37.411.750,00

ANEXO IV – DEMANDA ESTIMADA

LOTE 1 – REDE GOVERNO V																										
Órgão/Entidade	Unidade de Fornecimento	Quantidade Estimada Por Item																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
ADAB	Unidade	80	0	1	1	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AGERBA	Unidade	1	0	0	0	0	0	0	0	0	0	0	0	13	0	0	0	0	0	0	0	0	0	0	0	0
BAHIAFARMA	Unidade	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BAHIAGÁS	Unidade	0	0	0	0	0	32	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
CAR	Unidade	0	0	0	0	0	0	0	0	0	0	0	0	16	0	0	0	0	2	2	2	0	0	0	0	0
CBM	Unidade	32	0	0	0	32	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
CERB	Unidade	8	0	1	0	0	0	0	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CTB	Unidade	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
DETRAN	Unidade	148	0	0	0	0	0	0	0	0	0	5	0	0	5	0	0	24	32	16	0	0	0	0	0	0
DPE	Unidade	79	11	10	3	0	0	0	0	3	2	0	0	56	2	0	0	53	5	3	0	0	0	0	0	0
EGBA	Unidade	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FPC	Unidade	5	2	5	3	4	1	0	0	0	0	0	0	1	3	0	0	0	0	0	0	0	0	0	0	0
FUNDAC	Unidade	0	0	0	0	0	0	0	4	0	4	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
HEMOBA	Unidade	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0
IBAMETRO	Unidade	9	2	2	2	2	2	9	2	2	2	2	2	9	9	2	0	9	1	1	1	0	0	0	0	0
INEMA	Unidade	0	0	0	0	10	0	0	0	30	0	0	0	0	0	0	0	0	5	5	5	0	0	0	0	0
MPBA	Unidade	0	62	7	45	3	0	17	0	20	0	40	0	0	0	0	0	140	15	20	15	0	0	0	0	0
PC	Unidade	253	0	8	36	0	0	0	0	0	0	0	0	0	0	0	0	0	12	12	8	0	0	0	0	0
PGE	Unidade	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	1	3	2	0	0	0	0	0
PMBA	Unidade	112	16	40	8	0	16	0	0	0	0	0	0	0	0	0	0	91	2	3	3	0	0	0	0	0
SAEB/SAC	Unidade	0	48	0	8	0	40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SDE	Unidade	2	0	0	0	1	0	0	0	0	0	0	0	2	0	0	0	1	0	2	0	0	0	0	0	0
SDR/BAHIATER	Unidade	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SEADES	Unidade	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0
SEAP	Unidade	0	0	0	15	0	0	16	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0
SEBRAE	Unidade	0	0	0	0	0	0	0	0	1	0	0	0	0	28	0	0	0	13	8	1	0	0	0	0	0
SEC	Unidade	740	480	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SECTI	Unidade	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
SECULT	Unidade	15	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SEFAZ	Unidade	26	0	0	2	10	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0
SESAB	Unidade	5	37	5	16	16	10	5	8	8	4	34	5	5	8	8	16	5	8	8	8	0	0	0	0	0
SETRE	Unidade	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	45	5	5	5	0	0	0	0	0
SSP/DPT	Unidade	16	16	0	10	5	0	0	0	10	10	0	0	0	0	5	0	0	10	8	8	0	0	0	0	0

SSP/SGTO	Unidade	0	0	24	0	32	0	0	0	0	0	0	0	0	0	0	0	0	24	24	24	0	0	0	0	0
SSP/SI	Unidade	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SSP/STELECOM	Unidade	0	0	0	18	12	0	0	0	0	0	0	0	0	0	0	0	0	3	2	6	0	0	0	0	0
SUDEC	Unidade	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
SUDESB	Unidade	0	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
TCM	Unidade	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16	0	1	1	0	0	0	0	0
UEFS	Unidade	0	0	0	0	2	0	5	1	3	5	4	1	0	0	0	0	0	1	1	0	0	0	0	0	0
UESB	Unidade	0	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
UESC	Unidade	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
UNEB	Unidade	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PRODEB	Unidade	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	2	50	4	5.000
Quantidade Total Por Item		1589	707	109	167	149	101	54	16	78	33	91	14	105	50	20	16	369	137	144	108	10	2	50	4	5.000

LOTE 2 – SOLUÇÕES DE SEGURANÇA														
Item	Unidade de Fornecimento	Quantidade Estimada Por Órgão/Entidade												Quantidade Total
		Casa Civil	Casa Militar	DETRAN	EGBA	PMBA	PRODEB	SEAP	SEC	SEFAZ	SESAB	SETRE	SSP	
1	Unidade	0	0	0	0	0	0	0	0	0	2	0	2	4
2	Unidade	0	0	0	0	0	0	0	0	4	0	0	0	4
3	Unidade	0	0	0	0	4	0	0	0	0	0	0	4	8
4	Unidade	0	0	0	0	0	0	0	0	0	0	0	9	9
5	Unidade	4	0	0	0	0	0	0	0	0	0	0	0	4
6	Unidade	0	0	0	0	0	0	0	24	0	0	0	0	24
7	Unidade	0	0	0	0	0	0	0	0	0	12	0	0	12
8	Unidade	0	0	220	0	0	20	0	0	0	60	0	0	300
9	Unidade	0	0	0	0	0	0	0	300	0	0	0	0	300
10	Unidade	0	2	1	0	0	0	0	0	0	0	1	0	4
11	Unidade	0	0	0	0	2	0	2	0	0	0	0	0	4
12	Unidade	0	0	0	0	0	0	0	0	0	4	0	0	4
13	Unidade	0	0	0	0	0	2	0	0	0	2	0	0	4
14	Unidade	0	0	0	0	0	2	0	0	0	2	0	0	4
15	Unidade	0	0	0	0	0	4	0	0	0	0	0	0	4
16	Unidade	0	0	0	0	0	4	0	0	0	0	0	0	4

17	Unidade	0	0	0	0	0	2	0	0	0	0	0	0	2
18	Unidade	0	0	0	0	0	4	0	0	0	0	0	0	4
19	Unidade	0	0	0	0	0	60	0	0	0	0	0	0	60
20	Unidade	0	0	0	0	0	2	0	0	0	0	0	0	2
21	Unidade	0	0	0	0	0	4	0	0	0	0	0	0	4
22	Unidade	0	0	0	0	0	2	0	0	0	0	0	0	2
23	Unidade	0	0	0	0	0	2	0	0	0	0	0	0	2
24	Unidade	0	0	0	0	0	2	0	0	0	0	0	0	2
25	Unidade	0	0	0	0	0	4	0	0	0	0	0	0	4
26	Unidade	0	0	0	0	0	2	0	0	0	0	0	0	2
27	Unidade	0	0	0	0	0	2	0	0	0	0	0	0	2
28	Unidade	0	0	0	0	0	10	0	0	0	0	0	0	10
29	Unidade	0	0	0	0	0	10	0	0	0	0	0	0	10
30	Unidade	0	0	0	0	0	10	0	0	0	0	0	0	10
31	Unidade	0	0	0	0	0	10	0	0	0	0	0	0	10
32	Unidade	0	0	0	0	0	6	0	0	0	0	0	0	6
33	Unidade	0	0	0	0	0	6	0	0	0	0	0	0	6
34	Unidade	0	0	0	0	0	100	0	0	0	0	0	0	100
35	Unidade	0	0	0	0	0	100	0	0	0	0	0	0	100
36	Unidade	0	0	0	0	0	50	0	0	0	0	0	0	50
37	Unidade	0	0	0	0	0	50	0	0	0	0	0	0	50

ANEXO - ESPECIFICAÇÃO TÉCNICA DOS ITENS

LOTE 01

1. LOTE 01 - ITEM 01 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 01

- 1.1. A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 01 deve ser implantada em unidades governamentais que necessitam de conectividade segura, proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, um link de internet banda larga, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:
- 1.2. SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW
 - 1.2.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.
 - 1.2.2. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance físico), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;
 - 1.2.3. Poderá ser feita composição de soluções para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
 - 1.2.4. A solução deve permitir acesso a gerência e monitoramento, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
 - 1.2.5. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.
 - 1.2.6. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
 - 1.2.7. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN,

Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.

- 1.2.8. Deve suportar e estar licenciado para a criação de, ao menos, 10 (dez) instâncias virtuais de firewall no mesmo hardware.
- 1.2.9. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 1.2.10. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 1.2.11. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 1.2.12. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 1.2.13. Deve possuir firewall com capacidade mínima de processamento de 6 (seis) Gbps.
- 1.2.14. Deve possuir IPS com capacidade mínima de processamento de 1 (um) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 1.2.15. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1,2 (um virgula dois) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 1.2.16. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 1,3 (um virgula três) Gbps.
- 1.2.17. Deve possuir VPN com capacidade de, pelo menos, 06 (seis) Gbps de tráfego IPSec.
- 1.2.18. Deve suportar 1.000.000 (um milhão) conexões simultâneas.
- 1.2.19. Deve suportar, pelo menos, 100.000 (cem mil) novas conexões por segundo.
- 1.2.20. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.
- 1.2.21. Deve suportar, pelo menos, 450 (quatrocentos e cinquenta) túneis de VPN Client-Site.
- 1.2.22. Deve possuir, pelo menos, 09 (nove) interfaces RJ45 1GE.

- 1.2.23. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 1.2.24. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 1.2.25. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.
- 1.2.26. FUNCIONALIDADES DE FIREWALL
- 1.2.26.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
- 1.2.26.2. Possuir suporte a sub-interfaces ethernet lógicas;
- 1.2.26.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
- 1.2.26.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
- 1.2.26.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 1.2.26.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 1.2.26.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 1.2.26.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 1.2.26.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 1.2.26.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 1.2.26.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 1.2.26.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 1.2.26.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 1.2.26.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 1.2.26.15. Deve suportar o encaminhamento de tráfego multicast.

- 1.2.26.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 1.2.26.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 1.2.26.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 1.2.26.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 1.2.26.20. Suportar OSPF graceful restart;
- 1.2.26.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 1.2.26.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 1.2.26.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 1.2.26.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 1.2.26.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 1.2.26.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 1.2.26.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 1.2.26.28. Drop sem notificação do bloqueio ao usuário;
 - 1.2.26.29. Drop com notificação do bloqueio ao usuário;
 - 1.2.26.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 1.2.26.31. TCP-Reset para o cliente;
 - 1.2.26.32. TCP-Reset para o server ou para os dois lados da conexão.
- 1.2.26.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 1.2.26.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 1.2.26.35. Deve oferecer suporte ao protocolo SIP.
- 1.2.26.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.

- 1.2.26.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 1.2.26.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 1.2.26.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 1.2.26.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 1.2.26.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 1.2.26.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 1.2.26.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 1.2.26.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 1.2.26.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.2.26.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 1.2.26.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 1.2.26.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 1.2.26.49. Realizar Traffic Shaping para a solução de segurança
- 1.2.26.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 1.2.26.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 1.2.26.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;

- 1.2.26.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 1.2.26.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 1.2.26.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 1.2.26.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 1.2.26.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 1.2.26.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 1.2.26.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 1.2.26.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 1.2.26.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 1.2.26.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 1.2.26.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 1.2.26.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 1.2.26.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 1.2.26.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 1.2.26.67. Funcionar com tradução de porta (PAT);
- 1.2.26.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 1.2.26.69. Implementar e suportar NAT64 e NAT46;
- 1.2.26.70. Implementar NAT66
- 1.2.26.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 1.2.26.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 1.2.26.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-

Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.

1.2.26.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.

1.2.26.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:

1.2.26.75.1. Conectores SDN Privados:

- 1.2.26.75.1.1. Nutanix;
- 1.2.26.75.1.2. Kubernetes;
- 1.2.26.75.1.3. VMware ESXi;
- 1.2.26.75.1.4. OpenStack;

1.2.26.75.2. Conectores SDN Públicos;

- 1.2.26.75.2.1. Google Cloud Platform (GCP);
- 1.2.26.75.2.2. AWS;
- 1.2.26.75.2.3. Microsoft Azure;
- 1.2.26.75.2.4. Oracle Cloud Infrastructure (OCI);

1.2.26.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).

1.2.26.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;

1.2.26.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).

1.2.26.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.

1.2.26.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

1.2.27. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

- 1.2.27.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
- 1.2.27.2. Deve permitir modificação de valores DSCP para o DiffServ.
- 1.2.27.3. Deve permitir priorização de tráfego e suportar ToS.
- 1.2.27.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
- 1.2.27.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 1.2.27.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 1.2.27.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 1.2.27.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 1.2.27.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
- 1.2.27.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.
- 1.2.28. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB
 - 1.2.28.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
 - 1.2.28.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
 - 1.2.28.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
 - 1.2.28.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
 - 1.2.28.5. Deve permitir a criação de categorias personalizadas.
 - 1.2.28.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
 - 1.2.28.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
 - 1.2.28.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.

- 1.2.28.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 1.2.28.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 1.2.28.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 1.2.28.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 1.2.28.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 1.2.28.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 1.2.28.15. Permitir a criação de categorias de URLs customizadas;
- 1.2.28.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 1.2.28.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 1.2.28.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 1.2.28.19. Permitir a customização de página de bloqueio;
- 1.2.28.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 1.2.28.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 1.2.28.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 1.2.28.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 1.2.28.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em

políticas definidas pela CONTRATANTE aderente;

- 1.2.28.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 1.2.28.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 1.2.28.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 1.2.28.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 1.2.28.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 1.2.28.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 1.2.28.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 1.2.28.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 1.2.28.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 1.2.28.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 1.2.28.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 1.2.28.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 1.2.28.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 1.2.28.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 1.2.28.39. Deve possuir Proxy Explícito e Transparente.
- 1.2.28.40. Deve implementar roteamento WCCP e ICAP.
- 1.2.29. **FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)**
 - 1.2.29.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
 - 1.2.29.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.

- 1.2.29.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 1.2.29.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 1.2.29.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 1.2.29.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 1.2.29.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 1.2.29.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 1.2.29.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 1.2.29.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 1.2.29.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 1.2.29.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 1.2.29.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 1.2.29.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 1.2.29.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 1.2.29.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 1.2.29.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 1.2.29.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).

- 1.2.29.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 1.2.29.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 1.2.29.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 1.2.29.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 1.2.29.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 1.2.29.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 1.2.29.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 1.2.29.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 1.2.29.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 1.2.29.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 1.2.29.29. Identificar, alertar e bloquear comunicação com botnets;
- 1.2.29.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 1.2.29.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 1.2.29.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 1.2.29.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 1.2.29.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições

de resolução de nome para domínios maliciosos de botnets conhecidas;

1.2.29.35. Identificar nos eventos o país de onde partiu a ameaça;

1.2.29.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;

1.2.29.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

1.2.29.38. Deve possuir alarmes na console de administração.

1.2.29.39. Deve possuir alertas via correio eletrônico.

1.2.29.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.

1.2.29.41. Deve ter a capacidade de resposta/logs ativa a ataques.

1.2.29.42. Incluir proteção contra ataques de negação de serviços (DoS);

1.2.29.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);

1.2.29.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

1.2.30. FUNCIONALIDADE DE VPN

1.2.30.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;

1.2.30.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;

1.2.30.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;

1.2.30.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;

1.2.30.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;

1.2.30.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);

1.2.30.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;

1.2.30.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);

1.2.30.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;

- 1.2.30.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 1.2.30.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 1.2.30.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 1.2.30.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 1.2.30.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 1.2.30.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 1.2.30.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 1.2.30.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSec estabelecidos.
- 1.2.31. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
 - 1.2.31.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
 - 1.2.31.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
 - 1.2.31.3. Atualizar a base de assinaturas de aplicações automaticamente;
 - 1.2.31.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
 - 1.2.31.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
 - 1.2.31.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
 - 1.2.31.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;

- 1.2.31.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 1.2.31.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 1.2.31.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 1.2.31.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 1.2.31.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 1.2.31.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 1.2.31.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 1.2.31.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 1.2.31.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 1.2.31.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 1.2.31.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 1.2.31.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 1.2.31.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 1.2.31.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.

- 1.2.31.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 1.2.31.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 1.2.31.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 1.2.31.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 1.2.31.26. Deve permitir criação de padrões de aplicação manualmente.
- 1.2.31.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 1.2.31.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 1.2.31.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 1.2.31.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;
- 1.2.32. FUNCIONALIDADE DE SD-WAN
 - 1.2.32.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
 - 1.2.32.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.
 - 1.2.32.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
 - 1.2.32.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
 - 1.2.32.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
 - 1.2.32.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
 - 1.2.32.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.

- 1.2.32.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 1.2.32.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 1.2.32.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 1.2.32.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 1.2.32.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
 - 1.2.32.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
 - 1.2.32.14. Passivo: uso do tráfego real para as medições;
 - 1.2.32.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 1.2.32.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 1.2.32.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 1.2.32.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 1.2.32.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 1.2.32.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar

os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;

- 1.2.32.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 1.2.32.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 1.2.32.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 1.2.32.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 1.2.32.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 1.2.32.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 1.2.32.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 1.2.32.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 1.2.32.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

1.3. LINK DE CONECTIVIDADE BANDA LARGA

- 1.3.1. O link de 500 Mbps Banda Larga serão fornecidos para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.
- 1.3.2. Deve ser utilizado link de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-

WAN.

- 1.3.3. Deve ser fornecido 01 (um) link de internet com velocidade mínima de 500 Mbps de download.
- 1.3.4. O link de internet Banda Larga fornecido deverá disponibilizar endereçamento IP fixo em IPv6, válido e roteável na Internet, atribuído exclusivamente ao CONTRATANTE, não sendo permitido o uso de endereçamento dinâmico, NAT ou CGNAT para o tráfego IPv6.
- 1.3.5. Deve suportar transporte de pacotes IPv4 e IPv6.
- 1.3.6. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 1.3.7. O link deve ser entregue e mantido sem restrições de volume de tráfego.
- 1.3.8. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 1.3.9. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 1.3.10. O link não poderá ter franquia de acesso que limite sua utilização.
- 1.3.11. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 1.3.12. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.
- 1.3.13. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 1.3.14. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 1.3.15. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 1.3.16. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 1.3.17. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 1.3.18. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 1.3.19. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 1.3.20. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem

tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

1.4. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

1.4.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:

- 1.4.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.
- 1.4.1.2. Ativação e testes de 01 Link de Internet Banda Larga , assegurando estabilidade e disponibilidade.
- 1.4.1.3. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

1.4.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas no Centro de Monitoramento e Controle, garantindo:

- 1.4.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.
- 1.4.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.
- 1.4.2.3. Gerenciamento remoto e centralizado das políticas de segurança de endpoint.
- 1.4.2.4. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

2. LOTE 01 - ITEM 02 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 02

2.1. A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 02 deve ser implantada em unidades governamentais que necessitam de conectividade segura, proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, dois links de internet banda larga, com integração total ao ambiente de gerenciamento centralizado.

2.2. SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW

- 2.2.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.
- 2.2.2. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma

arquitetura específica e dedicada (appliance), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;

- 2.2.3. Poderá ser feita composição de soluções para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 2.2.4. Garantir que a solução disponibilize no(s) equipamento(s), acesso a gerência e monitoração, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
- 2.2.5. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.
- 2.2.6. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
- 2.2.7. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.
- 2.2.8. Deve suportar e estar licenciado para a criação de, ao menos, 10(dez) instâncias virtuais de firewall no mesmo hardware.
- 2.2.9. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 2.2.10. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 2.2.11. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 2.2.12. Deve possuir fonte de alimentação com chaveamento automático 110/220V.

- 2.2.13. Deve possuir firewall com capacidade mínima de processamento de 6 (seis) Gbps.
- 2.2.14. Deve possuir IPS com capacidade mínima de processamento de 1 (um) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 2.2.15. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1,2 (um virgula dois) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 2.2.16. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 1,3 (um virgula três) Gbps.
- 2.2.17. Deve possuir VPN com capacidade de, pelo menos, 06 (seis) Gbps de tráfego IPSec.
- 2.2.18. Deve suportar 1.000.000 (um milhão) conexões simultâneas.
- 2.2.19. Deve suportar, pelo menos, 100.000 (cem mil) novas conexões por segundo.
- 2.2.20. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.
- 2.2.21. Deve suportar, pelo menos, 450 (quatrocentos e cinquenta) túneis de VPN Client-Site.
- 2.2.22. Deve possuir, pelo menos, 09 (nove) interfaces RJ45 1GE.
- 2.2.23. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 2.2.24. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 2.2.25. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.
- 2.2.26. FUNCIONALIDADES DE FIREWALL
 - 2.2.26.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
 - 2.2.26.2. Possuir suporte a sub-interfaces ethernet lógicas;
 - 2.2.26.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
 - 2.2.26.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.

- 2.2.26.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 2.2.26.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 2.2.26.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 2.2.26.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 2.2.26.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 2.2.26.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 2.2.26.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 2.2.26.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 2.2.26.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 2.2.26.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 2.2.26.15. Deve suportar o encaminhamento de tráfego multicast.
- 2.2.26.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 2.2.26.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 2.2.26.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 2.2.26.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 2.2.26.20. Suportar OSPF gracefulrestart;
- 2.2.26.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 2.2.26.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 2.2.26.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 2.2.26.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 2.2.26.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter

visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

2.2.26.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

2.2.26.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:

2.2.26.28. Drop sem notificação do bloqueio ao usuário;

2.2.26.29. Drop com notificação do bloqueio ao usuário;

2.2.26.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;

2.2.26.31. TCP-Reset para o cliente;

2.2.26.32. TCP-Reset para o server ou para os dois lados da conexão.

2.2.26.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

2.2.26.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

2.2.26.35. Deve oferecer suporte ao protocolo SIP.

2.2.26.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.

2.2.26.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.

2.2.26.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.

2.2.26.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.

2.2.26.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.

2.2.26.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.

2.2.26.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.

2.2.26.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.

2.2.26.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS

e TACACS +.

- 2.2.26.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.2.26.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 2.2.26.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 2.2.26.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 2.2.26.49. Realizar Traffic Shaping para a solução de segurança
- 2.2.26.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 2.2.26.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 2.2.26.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 2.2.26.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 2.2.26.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 2.2.26.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 2.2.26.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 2.2.26.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 2.2.26.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 2.2.26.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;

- 2.2.26.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 2.2.26.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 2.2.26.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 2.2.26.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 2.2.26.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 2.2.26.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 2.2.26.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 2.2.26.67. Funcionar com tradução de porta (PAT);
- 2.2.26.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 2.2.26.69. Implementar e suportar NAT64 e NAT46;
- 2.2.26.70. Implementar NAT66
- 2.2.26.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 2.2.26.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 2.2.26.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 2.2.26.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 2.2.26.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:
 - 2.2.26.75.1. Conectores SDN Privados:
 - 2.2.26.75.1.1. Nutanix;
 - 2.2.26.75.1.2. Kubernetes;
 - 2.2.26.75.1.3. VMware ESXi;

- 2.2.26.75.1.4. OpenStack;
- 2.2.26.75.2. Conectores SDN Públicos;
 - 2.2.26.75.2.1. Google Cloud Platform (GCP);
 - 2.2.26.75.2.2. AWS;
 - 2.2.26.75.2.3. Microsoft Azure;
 - 2.2.26.75.2.4. Oracle Cloud Infrastructure (OCI);
- 2.2.26.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 2.2.26.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 2.2.26.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).
- 2.2.26.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.
- 2.2.26.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.
- 2.2.27. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO
 - 2.2.27.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
 - 2.2.27.2. Deve permitir modificação de valores DSCP para o DiffServ.
 - 2.2.27.3. Deve permitir priorização de tráfego e suportar ToS.
 - 2.2.27.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
 - 2.2.27.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
 - 2.2.27.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
 - 2.2.27.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
 - 2.2.27.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de

IPs, protocolo e aplicação.

2.2.27.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.

2.2.27.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

2.2.28. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

2.2.28.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.

2.2.28.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.

2.2.28.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.

2.2.28.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

2.2.28.5. Deve permitir a criação de categorias personalizadas.

2.2.28.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.

2.2.28.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.

2.2.28.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.

2.2.28.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.

2.2.28.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;

2.2.28.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

2.2.28.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

2.2.28.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;

2.2.28.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

2.2.28.15. Permitir a criação de categorias de URLs customizadas;

2.2.28.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com

a opção Safe Search habilitada;

- 2.2.28.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 2.2.28.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 2.2.28.19. Permitir a customização de página de bloqueio;
- 2.2.28.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 2.2.28.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 2.2.28.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.2.28.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 2.2.28.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 2.2.28.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 2.2.28.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 2.2.28.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 2.2.28.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 2.2.28.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 2.2.28.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 2.2.28.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não

contenha um domínio válido.

2.2.28.32. Deve filtrar o conteúdo baseado em categorias em tempo real.

2.2.28.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.

2.2.28.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.

2.2.28.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.

2.2.28.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.

2.2.28.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.

2.2.28.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.

2.2.28.39. Deve possuir Proxy Explícito e Transparente.

2.2.28.40. Deve implementar roteamento WCCP e ICAP.

2.2.29. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)

2.2.29.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.

2.2.29.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.

2.2.29.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

2.2.29.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

2.2.29.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;

2.2.29.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;

2.2.29.7. Deve permitir funcionar em modo transparente, sniffer e router.

2.2.29.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.

2.2.29.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;

2.2.29.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de

monitoração;

- 2.2.29.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 2.2.29.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 2.2.29.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 2.2.29.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 2.2.29.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 2.2.29.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 2.2.29.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 2.2.29.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 2.2.29.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 2.2.29.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 2.2.29.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 2.2.29.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 2.2.29.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 2.2.29.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 2.2.29.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 2.2.29.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 2.2.29.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas

de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;

- 2.2.29.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 2.2.29.29. Identificar, alertar e bloquear comunicação com botnets;
- 2.2.29.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 2.2.29.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 2.2.29.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 2.2.29.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 2.2.29.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 2.2.29.35. Identificar nos eventos o país de onde partiu a ameaça;
- 2.2.29.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 2.2.29.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 2.2.29.38. Deve possuir alarmes na console de administração.
- 2.2.29.39. Deve possuir alertas via correio eletrônico.
- 2.2.29.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 2.2.29.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 2.2.29.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 2.2.29.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);

2.2.29.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

2.2.30. FUNCIONALIDADE DE VPN

2.2.30.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;

2.2.30.2. Suportar nativamente a criação de VPN IPsec utilizando 3DES;

2.2.30.3. Suportar nativamente a criação de VPN IPsec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;

2.2.30.4. Suportar nativamente a autenticação de VPN IPsec utilizando MD5 e SHA-1;

2.2.30.5. Suportar nativamente a criação de VPN IPsec utilizando o algoritmo Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

2.2.30.6. Suportar nativamente a criação de VPN IPsec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);

2.2.30.7. Suportar nativamente, para VPN IPsec, autenticação via certificado IKE PKI;

2.2.30.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPsec a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);

2.2.30.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;

2.2.30.10. Realizar atribuição de DNS nos clientes remotos de VPN;

2.2.30.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;

2.2.30.12. Suportar leitura e verificação de CRL (Certificate Revocation List);

2.2.30.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;

2.2.30.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;

2.2.30.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;

2.2.30.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.

2.2.30.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPsec estabelecidos.

2.2.31. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

- 2.2.31.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
- 2.2.31.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
- 2.2.31.3. Atualizar a base de assinaturas de aplicações automaticamente;
- 2.2.31.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
- 2.2.31.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 2.2.31.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 2.2.31.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 2.2.31.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 2.2.31.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 2.2.31.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 2.2.31.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 2.2.31.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 2.2.31.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 2.2.31.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.

- 2.2.31.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 2.2.31.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 2.2.31.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 2.2.31.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 2.2.31.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 2.2.31.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 2.2.31.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 2.2.31.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 2.2.31.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 2.2.31.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 2.2.31.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 2.2.31.26. Deve permitir criação de padrões de aplicação manualmente.
- 2.2.31.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 2.2.31.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 2.2.31.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 2.2.31.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia

proprietária;

2.2.32. FUNCIONALIDADE DE SD-WAN

- 2.2.32.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
- 2.2.32.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.
- 2.2.32.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 2.2.32.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 2.2.32.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 2.2.32.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 2.2.32.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 2.2.32.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 2.2.32.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 2.2.32.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 2.2.32.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 2.2.32.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 2.2.32.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;

- 2.2.32.14. Passivo: uso do tráfego real para as medições;
- 2.2.32.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 2.2.32.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 2.2.32.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 2.2.32.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 2.2.32.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 2.2.32.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 2.2.32.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 2.2.32.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 2.2.32.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 2.2.32.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 2.2.32.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de

banda é modificada;

- 2.2.32.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 2.2.32.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 2.2.32.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 2.2.32.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

2.3. LINK DE CONECTIVIDADE BANDA LARGA EM DUPLA ABORDAGEM

- 2.3.1. Deve ser fornecidos dois links de 500 Mbps Banda Larga cada, para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.
- 2.3.2. Deve ser utilizados links de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.
- 2.3.3. Deve ser fornecido 02 (dois) link de internet com velocidade mínima de 500 Mbps de download cada.
- 2.3.4. Os circuitos de internet terrestre em cada unidade deverão ser entregues cada um por uma operadora ou provedor exclusivo.
- 2.3.5. Os links devem ser estabelecidos por caminhos completamente distintos, não devendo haver nenhum ponto de falha comum entre os dois links de comunicação.
- 2.3.6. Os links de internet Banda Larga fornecidos deverão disponibilizar endereçamento IP fixo em IPv6, válido e roteável na Internet, atribuído exclusivamente ao CONTRATANTE, não sendo permitido o uso de endereçamento dinâmico, NAT ou CGNAT para o tráfego IPv6.
- 2.3.7. Deve suportar transporte de pacotes IPv4 e IPv6.
- 2.3.8. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 2.3.9. O link deve ser entregue e mantido sem restrições de volume de tráfego.

- 2.3.10. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 2.3.11. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 2.3.12. O link não poderá ter franquia de acesso que limite sua utilização.
- 2.3.13. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 2.3.14. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.
- 2.3.15. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 2.3.16. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 2.3.17. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 2.3.18. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 2.3.19. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 2.3.20. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 2.3.21. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 2.3.22. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

2.4. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

- 2.4.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:
 - 2.4.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.
 - 2.4.1.2. Ativação e testes de 02 Links de Internet Banda Larga , assegurando estabilidade e disponibilidade.

- 2.4.1.3. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.
- 2.4.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:
 - 2.4.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.
 - 2.4.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.
 - 2.4.2.3. Gerenciamento remoto e centralizado das políticas de segurança de endpoint.
 - 2.4.2.4. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

3. LOTE 01 - ITEM 03 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 03

- 3.1. A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 03 deve ser implantada em unidades governamentais que necessitam de conectividade segura, proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, um link de internet banda larga, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:
- 3.2. SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW
 - 3.2.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.
 - 3.2.2. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance físico), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;
 - 3.2.3. Poderá ser feita composição de soluções para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
 - 3.2.4. A solução deve permitir acesso a gerência e monitoramento, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
 - 3.2.5. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-

ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.

- 3.2.6. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
- 3.2.7. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.
- 3.2.8. Deve suportar e estar licenciado para a criação de, ao menos, 10 (dez) instâncias virtuais de firewall no mesmo hardware.
- 3.2.9. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 3.2.10. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 3.2.11. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 3.2.12. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 3.2.13. Deve possuir firewall com capacidade mínima de processamento de 26 (vinte e seis) Gbps.
- 3.2.14. Deve possuir IPS com capacidade mínima de processamento de 5 (cinco) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 3.2.15. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 2,5 (dois vírgula cinco) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública,

disponível no site do fabricante.

- 3.2.16. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 3 (três) Gbps.
- 3.2.17. Deve possuir VPN com capacidade de, pelo menos, 33 (trinta e três) Gbps de tráfego IPSec.
- 3.2.18. Deve suportar 3.000.000 (três milhões) conexões simultâneas.
- 3.2.19. Deve suportar, pelo menos, 135.000 (cento e trinta e cinco mil) novas conexões por segundo.
- 3.2.20. Deve suportar, pelo menos, 1800 (mil e oitocentos) túneis de VPN Site-Site.
- 3.2.21. Deve suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site.
- 3.2.22. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE.
- 3.2.23. Deve possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE.
- 3.2.24. Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.
- 3.2.25. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 3.2.26. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 3.2.27. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.
- 3.2.28. FUNCIONALIDADES DE FIREWALL
 - 3.2.28.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
 - 3.2.28.2. Possuir suporte a sub-interfaces ethernet lógicas;
 - 3.2.28.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
 - 3.2.28.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
 - 3.2.28.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
 - 3.2.28.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
 - 3.2.28.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);

- 3.2.28.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 3.2.28.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 3.2.28.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 3.2.28.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 3.2.28.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 3.2.28.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 3.2.28.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 3.2.28.15. Deve suportar o encaminhamento de tráfego multicast.
- 3.2.28.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 3.2.28.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 3.2.28.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 3.2.28.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 3.2.28.20. Suportar OSPF gracefulrestart;
- 3.2.28.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 3.2.28.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 3.2.28.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 3.2.28.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 3.2.28.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 3.2.28.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 3.2.28.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 3.2.28.28. Drop sem notificação do bloqueio ao usuário;

- 3.2.28.29. Drop com notificação do bloqueio ao usuário;
- 3.2.28.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
- 3.2.28.31. TCP-Reset para o cliente;
- 3.2.28.32. TCP-Reset para o server ou para os dois lados da conexão.
- 3.2.28.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 3.2.28.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 3.2.28.35. Deve oferecer suporte ao protocolo SIP.
- 3.2.28.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 3.2.28.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 3.2.28.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 3.2.28.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 3.2.28.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 3.2.28.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 3.2.28.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 3.2.28.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 3.2.28.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 3.2.28.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 3.2.28.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de

usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;

- 3.2.28.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 3.2.28.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 3.2.28.49. Realizar Traffic Shaping para a solução de segurança
- 3.2.28.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 3.2.28.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 3.2.28.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 3.2.28.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 3.2.28.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 3.2.28.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 3.2.28.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 3.2.28.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 3.2.28.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 3.2.28.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 3.2.28.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 3.2.28.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 3.2.28.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 3.2.28.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).

- 3.2.28.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 3.2.28.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 3.2.28.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 3.2.28.67. Funcionar com tradução de porta (PAT);
- 3.2.28.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 3.2.28.69. Implementar e suportar NAT64 e NAT46;
- 3.2.28.70. Implementar NAT66
- 3.2.28.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 3.2.28.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 3.2.28.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 3.2.28.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 3.2.28.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:
 - 3.2.28.75.1. Conectores SDN Privados:
 - 3.2.28.75.1.1. Nutanix;
 - 3.2.28.75.1.2. Kubernetes;
 - 3.2.28.75.1.3. VMware ESXi;
 - 3.2.28.75.1.4. OpenStack;
 - 3.2.28.75.2. Conectores SDN Públicos;
 - 3.2.28.75.2.1. Google Cloud Platform (GCP);
 - 3.2.28.75.2.2. AWS;
 - 3.2.28.75.2.3. Microsoft Azure;
 - 3.2.28.75.2.4. Oracle Cloud Infrastructure (OCI);

- 3.2.28.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 3.2.28.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 3.2.28.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).
- 3.2.28.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.
- 3.2.28.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.
- 3.2.29. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO
 - 3.2.29.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
 - 3.2.29.2. Deve permitir modificação de valores DSCP para o DiffServ.
 - 3.2.29.3. Deve permitir priorização de tráfego e suportar ToS.
 - 3.2.29.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
 - 3.2.29.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
 - 3.2.29.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
 - 3.2.29.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
 - 3.2.29.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
 - 3.2.29.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
 - 3.2.29.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.
- 3.2.30. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

- 3.2.30.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
- 3.2.30.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
- 3.2.30.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
- 3.2.30.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 3.2.30.5. Deve permitir a criação de categorias personalizadas.
- 3.2.30.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 3.2.30.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 3.2.30.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 3.2.30.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 3.2.30.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 3.2.30.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 3.2.30.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 3.2.30.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 3.2.30.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 3.2.30.15. Permitir a criação de categorias de URLs customizadas;
- 3.2.30.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 3.2.30.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 3.2.30.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 3.2.30.19. Permitir a customização de página de bloqueio;
- 3.2.30.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem

está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;

- 3.2.30.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 3.2.30.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 3.2.30.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 3.2.30.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 3.2.30.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 3.2.30.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 3.2.30.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 3.2.30.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 3.2.30.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 3.2.30.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 3.2.30.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 3.2.30.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 3.2.30.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 3.2.30.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.

- 3.2.30.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 3.2.30.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 3.2.30.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 3.2.30.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 3.2.30.39. Deve possuir Proxy Explícito e Transparente.
- 3.2.30.40. Deve implementar roteamento WCCP e ICAP.
- 3.2.31. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)
 - 3.2.31.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
 - 3.2.31.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
 - 3.2.31.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
 - 3.2.31.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
 - 3.2.31.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
 - 3.2.31.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
 - 3.2.31.7. Deve permitir funcionar em modo transparente, sniffer e router.
 - 3.2.31.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
 - 3.2.31.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
 - 3.2.31.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
 - 3.2.31.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
 - 3.2.31.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
 - 3.2.31.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques,

baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);

- 3.2.31.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 3.2.31.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 3.2.31.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque.
Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 3.2.31.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 3.2.31.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 3.2.31.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 3.2.31.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 3.2.31.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 3.2.31.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões; Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 3.2.31.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 3.2.31.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 3.2.31.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 3.2.31.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 3.2.31.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 3.2.31.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 3.2.31.29. Identificar, alertar e bloquear comunicação com botnets;
- 3.2.31.30. Registrar na console de monitoração as seguintes informações sobre ameaças

identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

- 3.2.31.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 3.2.31.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 3.2.31.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 3.2.31.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 3.2.31.35. Identificar nos eventos o país de onde partiu a ameaça;
- 3.2.31.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 3.2.31.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 3.2.31.38. Deve possuir alarmes na console de administração.
- 3.2.31.39. Deve possuir alertas via correio eletrônico.
- 3.2.31.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 3.2.31.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 3.2.31.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 3.2.31.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 3.2.31.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;
- 3.2.32. FUNCIONALIDADE DE VPN
 - 3.2.32.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
 - 3.2.32.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;

- 3.2.32.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
- 3.2.32.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
- 3.2.32.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
- 3.2.32.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
- 3.2.32.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
- 3.2.32.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 3.2.32.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 3.2.32.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 3.2.32.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 3.2.32.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 3.2.32.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 3.2.32.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 3.2.32.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 3.2.32.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 3.2.32.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSec estabelecidos.
- 3.2.33. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
 - 3.2.33.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
 - 3.2.33.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do

protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;

- 3.2.33.3. Atualizar a base de assinaturas de aplicações automaticamente;
- 3.2.33.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
- 3.2.33.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 3.2.33.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 3.2.33.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 3.2.33.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 3.2.33.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 3.2.33.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 3.2.33.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 3.2.33.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensagens instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 3.2.33.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 3.2.33.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 3.2.33.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 3.2.33.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia

utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.

- 3.2.33.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 3.2.33.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 3.2.33.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 3.2.33.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 3.2.33.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 3.2.33.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 3.2.33.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 3.2.33.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 3.2.33.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 3.2.33.26. Deve permitir criação de padrões de aplicação manualmente.
- 3.2.33.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 3.2.33.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 3.2.33.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 3.2.33.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;
- 3.2.34. FUNCIONALIDADE DE SD-WAN
 - 3.2.34.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
 - 3.2.34.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira

autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.

- 3.2.34.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 3.2.34.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 3.2.34.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 3.2.34.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 3.2.34.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 3.2.34.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 3.2.34.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 3.2.34.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 3.2.34.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 3.2.34.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
 - 3.2.34.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
 - 3.2.34.14. Passivo: uso do tráfego real para as medições;
 - 3.2.34.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 3.2.34.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;

- 3.2.34.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 3.2.34.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 3.2.34.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 3.2.34.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 3.2.34.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 3.2.34.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 3.2.34.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 3.2.34.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 3.2.34.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 3.2.34.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 3.2.34.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-

WAN;

- 3.2.34.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 3.2.34.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

3.3. LINK DE CONECTIVIDADE BANDA LARGA

- 3.3.1. O link de 1 Gbps Banda Larga serão fornecidos para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.
- 3.3.2. Deve ser utilizado link de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.
- 3.3.3. Deve ser fornecido 01 (um) link de internet com velocidade mínima de 1 Gbps de download.
- 3.3.4. Para os locais em que não houver viabilidade técnica da CONTRATADA disponibilizar um link de internet com capacidade de 1 (um) Gbps, será admitida, mediante justificativa técnica, a entrega de 2 (dois) links distintos com capacidade mínima de 500 (quinhentos) Mbps cada, de forma a garantir a capacidade total equivalente.
- 3.3.5. O link de internet Banda Larga fornecido deverá disponibilizar endereçamento IP fixo em IPv6, válido e roteável na Internet, atribuído exclusivamente ao CONTRATANTE, não sendo permitido o uso de endereçamento dinâmico, NAT ou CGNAT para o tráfego IPv6.
- 3.3.6. Deve suportar transporte de pacotes IPv4 e IPv6.
- 3.3.7. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 3.3.8. O link deve ser entregue e mantido sem restrições de volume de tráfego.
- 3.3.9. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 3.3.10. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 3.3.11. O link não poderá ter franquia de acesso que limite sua utilização.
- 3.3.12. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 3.3.13. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.

- 3.3.14. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 3.3.15. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 3.3.16. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 3.3.17. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 3.3.18. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 3.3.19. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 3.3.20. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 3.3.21. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

3.4.IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

- 3.4.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:
 - 3.4.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.
 - 3.4.1.2. Ativação e testes de 01 Link de Internet Banda Larga , assegurando estabilidade e disponibilidade.
 - 3.4.1.3. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.
- 3.4.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:
 - 3.4.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.
 - 3.4.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo

análise de eventos e auditoria.

3.4.2.3. Gerenciamento remoto e centralizado das políticas de segurança de endpoint.

3.4.2.4. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

4. LOTE 01 - ITEM 04 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 04

4.1. A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 04 deve ser implantada em unidades governamentais que necessitam de conectividade segura, proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, dois links de internet banda larga, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

4.2. SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW

- 4.2.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.
- 4.2.2. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;
- 4.2.3. Poderá ser feita composição de soluções para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 4.2.4. Garantir que a solução disponibilize no(s) equipamento(s), acesso a gerência e monitoração, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
- 4.2.5. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem

apenas os equipamentos operando em alta disponibilidade.

- 4.2.6. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
- 4.2.7. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.
- 4.2.8. Deve suportar e estar licenciado para a criação de, ao menos 10(dez) instâncias virtuais de firewall no mesmo hardware.
- 4.2.9. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 4.2.10. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 4.2.11. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 4.2.12. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 4.2.13. Deve possuir firewall com capacidade mínima de processamento de 26 (vinte e seis) Gbps.
- 4.2.14. Deve possuir IPS com capacidade mínima de processamento de 5 (cinco) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 4.2.15. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 2,5 (dois vírgula cinco) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 4.2.16. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 3 (três) Gbps.
- 4.2.17. Deve possuir VPN com capacidade de, pelo menos, 33 (trinta e três) Gbps de tráfego

IPSec.

- 4.2.18. Deve suportar 3.000.000 (três milhões) conexões simultâneas.
- 4.2.19. Deve suportar, pelo menos, 135.000 (cento e trinta e cinco mil) novas conexões por segundo.
- 4.2.20. Deve suportar, pelo menos, 1800 (mil e oitocentos) túneis de VPN Site-Site.
- 4.2.21. Deve suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site.
- 4.2.22. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE.
- 4.2.23. Deve possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE.
- 4.2.24. Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.
- 4.2.25. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 4.2.26. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 4.2.27. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.
- 4.2.28. FUNCIONALIDADES DE FIREWALL
 - 4.2.28.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
 - 4.2.28.2. Possuir suporte a sub-interfaces ethernet lógicas;
 - 4.2.28.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
 - 4.2.28.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
 - 4.2.28.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
 - 4.2.28.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
 - 4.2.28.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
 - 4.2.28.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
 - 4.2.28.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
 - 4.2.28.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões

previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.

- 4.2.28.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 4.2.28.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 4.2.28.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 4.2.28.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 4.2.28.15. Deve suportar o encaminhamento de tráfego multicast.
- 4.2.28.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 4.2.28.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 4.2.28.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 4.2.28.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 4.2.28.20. Suportar OSPF gracefulrestart;
- 4.2.28.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 4.2.28.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 4.2.28.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 4.2.28.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 4.2.28.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 4.2.28.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 4.2.28.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 4.2.28.28. Drop sem notificação do bloqueio ao usuário;
 - 4.2.28.29. Drop com notificação do bloqueio ao usuário;
 - 4.2.28.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 4.2.28.31. TCP-Reset para o cliente;
 - 4.2.28.32. TCP-Reset para o server ou para os dois lados da conexão.

- 4.2.28.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 4.2.28.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 4.2.28.35. Deve oferecer suporte ao protocolo SIP.
- 4.2.28.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 4.2.28.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 4.2.28.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 4.2.28.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 4.2.28.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 4.2.28.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 4.2.28.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 4.2.28.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 4.2.28.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 4.2.28.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 4.2.28.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 4.2.28.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD,

sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;

- 4.2.28.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 4.2.28.49. Realizar Traffic Shaping para a solução de segurança
- 4.2.28.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 4.2.28.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 4.2.28.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 4.2.28.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 4.2.28.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 4.2.28.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 4.2.28.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 4.2.28.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 4.2.28.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 4.2.28.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 4.2.28.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 4.2.28.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 4.2.28.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 4.2.28.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 4.2.28.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 4.2.28.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);

- 4.2.28.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 4.2.28.67. Funcionar com tradução de porta (PAT);
- 4.2.28.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 4.2.28.69. Implementar e suportar NAT64 e NAT46;
- 4.2.28.70. Implementar NAT66
- 4.2.28.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 4.2.28.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 4.2.28.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 4.2.28.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 4.2.28.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:
 - 4.2.28.75.1. Conectores SDN Privados:
 - 4.2.28.75.1.1. Nutanix;
 - 4.2.28.75.1.2. Kubernetes;
 - 4.2.28.75.1.3. VMware ESXi;
 - 4.2.28.75.1.4. OpenStack;
 - 4.2.28.75.2. Conectores SDN Públicos;
 - 4.2.28.75.2.1. Google Cloud Platform (GCP);
 - 4.2.28.75.2.2. AWS;
 - 4.2.28.75.2.3. Microsoft Azure;
 - 4.2.28.75.2.4. Oracle Cloud Infrastructure (OCI);
- 4.2.28.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 4.2.28.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das

seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;

4.2.28.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).

4.2.28.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.

4.2.28.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

4.2.29. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

4.2.29.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.

4.2.29.2. Deve permitir modificação de valores DSCP para o DiffServ.

4.2.29.3. Deve permitir priorização de tráfego e suportar ToS.

4.2.29.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.

4.2.29.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.

4.2.29.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.

4.2.29.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.

4.2.29.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.

4.2.29.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.

4.2.29.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

4.2.30. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

4.2.30.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.

4.2.30.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.

4.2.30.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers,

Pornografia, Racismo, Websites pessoais, Compras.

- 4.2.30.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 4.2.30.5. Deve permitir a criação de categorias personalizadas.
- 4.2.30.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 4.2.30.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 4.2.30.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 4.2.30.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 4.2.30.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 4.2.30.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 4.2.30.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 4.2.30.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 4.2.30.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 4.2.30.15. Permitir a criação de categorias de URLs customizadas;
- 4.2.30.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 4.2.30.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 4.2.30.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 4.2.30.19. Permitir a customização de página de bloqueio;
- 4.2.30.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 4.2.30.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de

usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;

- 4.2.30.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 4.2.30.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 4.2.30.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 4.2.30.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 4.2.30.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 4.2.30.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 4.2.30.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 4.2.30.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 4.2.30.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 4.2.30.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 4.2.30.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 4.2.30.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 4.2.30.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 4.2.30.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 4.2.30.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 4.2.30.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.

4.2.30.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.

4.2.30.39. Deve possuir Proxy Explícito e Transparente.

4.2.30.40. Deve implementar roteamento WCCP e ICAP.

4.2.31. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)

4.2.31.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.

4.2.31.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.

4.2.31.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

4.2.31.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

4.2.31.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;

4.2.31.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;

4.2.31.7. Deve permitir funcionar em modo transparente, sniffer e router.

4.2.31.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.

4.2.31.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;

4.2.31.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;

4.2.31.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;

4.2.31.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;

4.2.31.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);

4.2.31.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de

destino, serviço e a combinação de todos esses itens;

- 4.2.31.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 4.2.31.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque.
Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 4.2.31.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 4.2.31.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 4.2.31.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 4.2.31.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 4.2.31.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 4.2.31.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 4.2.31.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 4.2.31.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 4.2.31.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 4.2.31.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 4.2.31.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 4.2.31.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 4.2.31.29. Identificar, alertar e bloquear comunicação com botnets;
- 4.2.31.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 4.2.31.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do

ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

- 4.2.31.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 4.2.31.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 4.2.31.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 4.2.31.35. Identificar nos eventos o país de onde partiu a ameaça;
- 4.2.31.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 4.2.31.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 4.2.31.38. Deve possuir alarmes na console de administração.
- 4.2.31.39. Deve possuir alertas via correio eletrônico.
- 4.2.31.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 4.2.31.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 4.2.31.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 4.2.31.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 4.2.31.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;
- 4.2.32. FUNCIONALIDADE DE VPN
 - 4.2.32.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
 - 4.2.32.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
 - 4.2.32.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
 - 4.2.32.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
 - 4.2.32.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup

1, Group 2, Group 5 e Group 14;

- 4.2.32.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
- 4.2.32.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
- 4.2.32.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 4.2.32.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 4.2.32.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 4.2.32.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 4.2.32.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 4.2.32.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 4.2.32.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 4.2.32.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 4.2.32.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 4.2.32.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSEC estabelecidos.
- 4.2.33. **FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**
 - 4.2.33.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
 - 4.2.33.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
 - 4.2.33.3. Atualizar a base de assinaturas de aplicações automaticamente;

- 4.2.33.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
- 4.2.33.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 4.2.33.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 4.2.33.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 4.2.33.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 4.2.33.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 4.2.33.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 4.2.33.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 4.2.33.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensagens instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 4.2.33.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 4.2.33.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 4.2.33.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 4.2.33.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 4.2.33.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos

usuários.

- 4.2.33.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 4.2.33.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 4.2.33.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 4.2.33.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 4.2.33.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 4.2.33.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 4.2.33.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 4.2.33.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 4.2.33.26. Deve permitir criação de padrões de aplicação manualmente.
- 4.2.33.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 4.2.33.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 4.2.33.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 4.2.33.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;
- 4.2.34. FUNCIONALIDADE DE SD-WAN
 - 4.2.34.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
 - 4.2.34.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.
 - 4.2.34.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;

- 4.2.34.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 4.2.34.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 4.2.34.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 4.2.34.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 4.2.34.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 4.2.34.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 4.2.34.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 4.2.34.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 4.2.34.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
 - 4.2.34.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
 - 4.2.34.14. Passivo: uso do tráfego real para as medições;
 - 4.2.34.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 4.2.34.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 4.2.34.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 4.2.34.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser

realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

- 4.2.34.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 4.2.34.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 4.2.34.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 4.2.34.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 4.2.34.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 4.2.34.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 4.2.34.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 4.2.34.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 4.2.34.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 4.2.34.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 4.2.34.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único

overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

4.3. LINK DE CONECTIVIDADE BANDA LARGA EM DUPLA ABORDAGEM

- 4.3.1. Deve ser fornecidos dois links de 1 Gbps Banda Larga cada, para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.
- 4.3.2. Deve ser utilizados links de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.
- 4.3.3. Deve ser fornecido 02 (dois) links de internet com velocidade mínima de 1 Gbps de download cada.
- 4.3.4. Os circuitos de internet terrestre em cada unidade deverão ser entregues cada um por uma operadora ou provedor exclusivo.
- 4.3.5. Os links devem ser estabelecidos por caminhos completamente distintos, não devendo haver nenhum ponto de falha comum entre os dois links de comunicação.
- 4.3.6. Para os locais em que não houver viabilidade técnica da CONTRATADA disponibilizar um link de internet com capacidade de 1 (um) Gbps, será admitida, mediante justificativa técnica, a entrega de 2 (dois) links distintos com capacidade mínima de 500 (quinhentos) Mbps cada, de forma a garantir a capacidade total equivalente.
- 4.3.7. Os links de internet Banda Larga fornecidos deverão disponibilizar endereçamento IP fixo em IPv6, válido e roteável na Internet, atribuído exclusivamente ao CONTRATANTE, não sendo permitido o uso de endereçamento dinâmico, NAT ou CGNAT para o tráfego IPv6.
- 4.3.8. Deve suportar transporte de pacotes IPv4 e IPv6.
- 4.3.9. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 4.3.10. O link deve ser entregue e mantido sem restrições de volume de tráfego.
- 4.3.11. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 4.3.12. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 4.3.13. O link não poderá ter franquia de acesso que limite sua utilização.
- 4.3.14. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 4.3.15. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas

próprias ou fornecidas pela Contratada.

- 4.3.16. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 4.3.17. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 4.3.18. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 4.3.19. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 4.3.20. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 4.3.21. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 4.3.22. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 4.3.23. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

4.4. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

- 4.4.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:
 - 4.4.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.
 - 4.4.1.2. Ativação e testes de 02 Links de Internet Banda Larga, assegurando estabilidade e disponibilidade.
 - 4.4.1.3. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.
- 4.4.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:
 - 4.4.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.

- 4.4.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.
- 4.4.2.3. Gerenciamento remoto e centralizado das políticas de segurança de endpoint.
- 4.4.2.4. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

5. LOTE 01 - ITEM 05 - SOLUÇÃO DE CONECTIVIDADE SEGURA – TIPO 05

5.1. A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 05 deve ser implantada em unidades governamentais que necessitam de conectividade segura, proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, um link de internet via satélite, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

5.2. SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW

- 5.2.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.
- 5.2.2. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;
- 5.2.3. Poderá ser feita composição de soluções para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 5.2.4. Garantir que a solução disponibilize no(s) equipamento(s), acesso a gerência e monitoração, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
- 5.2.5. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou

standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.

- 5.2.6. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
- 5.2.7. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.
- 5.2.8. Deve suportar e estar licenciado para a criação de, ao menos, 10(dez) instâncias virtuais de firewall no mesmo hardware.
- 5.2.9. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 5.2.10. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 5.2.11. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 5.2.12. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 5.2.13. Deve possuir firewall com capacidade mínima de processamento de 6 (seis) Gbps.
- 5.2.14. Deve possuir IPS com capacidade mínima de processamento de 1 (um) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 5.2.15. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1,2 (um virgula dois) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 5.2.16. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 1,3 (um virgula três) Gbps.
- 5.2.17. Deve possuir VPN com capacidade de, pelo menos, 06 (seis) Gbps de tráfego IPsec.

- 5.2.18. Deve suportar 1.000.000 (um milhão) conexões simultâneas.
- 5.2.19. Deve suportar, pelo menos, 100.000 (cem mil) novas conexões por segundo.
- 5.2.20. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.
- 5.2.21. Deve suportar, pelo menos, 450 (quatrocentos e cinquenta) túneis de VPN Client-Site.
- 5.2.22. Deve possuir, pelo menos, 09 (nove) interfaces RJ45 1GE.
- 5.2.23. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 5.2.24. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 5.2.25. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.
- 5.2.26. FUNCIONALIDADES DE FIREWALL
 - 5.2.26.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
 - 5.2.26.2. Possuir suporte a sub-interfaces ethernet lógicas;
 - 5.2.26.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
 - 5.2.26.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
 - 5.2.26.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
 - 5.2.26.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
 - 5.2.26.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
 - 5.2.26.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
 - 5.2.26.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
 - 5.2.26.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
 - 5.2.26.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
 - 5.2.26.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada

(Inbound) e saída (Outbound);

- 5.2.26.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 5.2.26.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 5.2.26.15. Deve suportar o encaminhamento de tráfego multicast.
- 5.2.26.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 5.2.26.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 5.2.26.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 5.2.26.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 5.2.26.20. Suportar OSPF graceful restart;
- 5.2.26.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 5.2.26.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 5.2.26.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 5.2.26.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 5.2.26.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 5.2.26.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 5.2.26.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 5.2.26.28. Drop sem notificação do bloqueio ao usuário;
 - 5.2.26.29. Drop com notificação do bloqueio ao usuário;
 - 5.2.26.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 5.2.26.31. TCP-Reset para o cliente;
 - 5.2.26.32. TCP-Reset para o server ou para os dois lados da conexão.
- 5.2.26.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 5.2.26.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts,

envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

- 5.2.26.35. Deve oferecer suporte ao protocolo SIP.
- 5.2.26.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 5.2.26.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 5.2.26.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 5.2.26.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 5.2.26.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 5.2.26.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 5.2.26.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 5.2.26.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 5.2.26.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 5.2.26.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 5.2.26.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 5.2.26.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 5.2.26.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP

de origem, usuários e grupos do LDAP, LDAP/AD;

5.2.26.49. Realizar Traffic Shaping para a solução de segurança

5.2.26.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;

5.2.26.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;

5.2.26.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;

5.2.26.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);

5.2.26.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.

5.2.26.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.

5.2.26.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.

5.2.26.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

5.2.26.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;

5.2.26.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;

5.2.26.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;

5.2.26.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;

5.2.26.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.

5.2.26.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).

5.2.26.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.

5.2.26.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);

5.2.26.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);

5.2.26.67. Funcionar com tradução de porta (PAT);

5.2.26.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;

- 5.2.26.69. Implementar e suportar NAT64 e NAT46;
- 5.2.26.70. Implementar NAT66
- 5.2.26.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 5.2.26.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 5.2.26.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 5.2.26.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 5.2.26.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:
 - 5.2.26.75.1. Conectores SDN Privados:
 - 5.2.26.75.1.1. Nutanix;
 - 5.2.26.75.1.2. Kubernetes;
 - 5.2.26.75.1.3. VMware ESXi;
 - 5.2.26.75.1.4. OpenStack;
 - 5.2.26.75.2. Conectores SDN Públicos;
 - 5.2.26.75.2.1. Google Cloud Platform (GCP);
 - 5.2.26.75.2.2. AWS;
 - 5.2.26.75.2.3. Microsoft Azure;
 - 5.2.26.75.2.4. Oracle Cloud Infrastructure (OCI);
- 5.2.26.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 5.2.26.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 5.2.26.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento

de arquivos (P2P) e de mensagens instantâneas (IM).

5.2.26.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.

5.2.26.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

5.2.27. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

5.2.27.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.

5.2.27.2. Deve permitir modificação de valores DSCP para o DiffServ.

5.2.27.3. Deve permitir priorização de tráfego e suportar ToS.

5.2.27.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.

5.2.27.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.

5.2.27.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.

5.2.27.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.

5.2.27.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.

5.2.27.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.

5.2.27.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

5.2.28. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

5.2.28.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.

5.2.28.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.

5.2.28.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.

5.2.28.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

5.2.28.5. Deve permitir a criação de categorias personalizadas.

- 5.2.28.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 5.2.28.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 5.2.28.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 5.2.28.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 5.2.28.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 5.2.28.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 5.2.28.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 5.2.28.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 5.2.28.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 5.2.28.15. Permitir a criação de categorias de URLs customizadas;
- 5.2.28.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 5.2.28.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 5.2.28.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 5.2.28.19. Permitir a customização de página de bloqueio;
- 5.2.28.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 5.2.28.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;

- 5.2.28.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 5.2.28.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 5.2.28.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 5.2.28.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 5.2.28.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 5.2.28.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 5.2.28.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 5.2.28.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 5.2.28.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 5.2.28.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 5.2.28.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 5.2.28.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 5.2.28.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 5.2.28.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 5.2.28.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 5.2.28.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 5.2.28.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 5.2.28.39. Deve possuir Proxy Explícito e Transparente.

5.2.28.40. Deve implementar roteamento WCCP e ICAP.

5.2.29. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)

- 5.2.29.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
- 5.2.29.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
- 5.2.29.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 5.2.29.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 5.2.29.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 5.2.29.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 5.2.29.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 5.2.29.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 5.2.29.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 5.2.29.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 5.2.29.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 5.2.29.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 5.2.29.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 5.2.29.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 5.2.29.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 5.2.29.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque.

Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.

- 5.2.29.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 5.2.29.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 5.2.29.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 5.2.29.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 5.2.29.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 5.2.29.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 5.2.29.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 5.2.29.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 5.2.29.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 5.2.29.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 5.2.29.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 5.2.29.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 5.2.29.29. Identificar, alertar e bloquear comunicação com botnets;
- 5.2.29.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 5.2.29.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 5.2.29.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP),

em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;

- 5.2.29.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
 - 5.2.29.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
 - 5.2.29.35. Identificar nos eventos o país de onde partiu a ameaça;
 - 5.2.29.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
 - 5.2.29.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
 - 5.2.29.38. Deve possuir alarmes na console de administração.
 - 5.2.29.39. Deve possuir alertas via correio eletrônico.
 - 5.2.29.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
 - 5.2.29.41. Deve ter a capacidade de resposta/logs ativa a ataques.
 - 5.2.29.42. Incluir proteção contra ataques de negação de serviços (DoS);
 - 5.2.29.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
 - 5.2.29.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;
- 5.2.30. FUNCIONALIDADE DE VPN
- 5.2.30.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
 - 5.2.30.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
 - 5.2.30.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
 - 5.2.30.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
 - 5.2.30.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
 - 5.2.30.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);

- 5.2.30.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
- 5.2.30.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSec a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 5.2.30.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 5.2.30.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 5.2.30.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 5.2.30.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 5.2.30.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 5.2.30.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 5.2.30.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 5.2.30.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 5.2.30.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSec estabelecidos.
- 5.2.31. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
 - 5.2.31.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
 - 5.2.31.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
 - 5.2.31.3. Atualizar a base de assinaturas de aplicações automaticamente;
 - 5.2.31.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
 - 5.2.31.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de

aplicações em algumas regras;

- 5.2.31.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 5.2.31.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 5.2.31.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 5.2.31.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 5.2.31.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 5.2.31.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 5.2.31.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 5.2.31.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 5.2.31.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 5.2.31.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 5.2.31.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 5.2.31.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 5.2.31.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.

- 5.2.31.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 5.2.31.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 5.2.31.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 5.2.31.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 5.2.31.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 5.2.31.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 5.2.31.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 5.2.31.26. Deve permitir criação de padrões de aplicação manualmente.
- 5.2.31.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 5.2.31.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 5.2.31.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 5.2.31.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;
- 5.2.32. FUNCIONALIDADE DE SD-WAN
 - 5.2.32.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
 - 5.2.32.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.
 - 5.2.32.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
 - 5.2.32.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
 - 5.2.32.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em

contexto de saída (Nat Outbound) para um pool de IPs públicos;

- 5.2.32.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 5.2.32.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 5.2.32.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 5.2.32.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 5.2.32.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 5.2.32.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 5.2.32.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
 - 5.2.32.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
 - 5.2.32.14. Passivo: uso do tráfego real para as medições;
 - 5.2.32.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 5.2.32.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 5.2.32.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 5.2.32.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 5.2.32.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de

Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;

- 5.2.32.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 5.2.32.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 5.2.32.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 5.2.32.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 5.2.32.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 5.2.32.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 5.2.32.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 5.2.32.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 5.2.32.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 5.2.32.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

5.3. LINK DE CONECTIVIDADE BANDA LARGA

- 5.3.1. O link de satélite de 100 Mbps Banda Larga serão fornecidos para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.
- 5.3.2. Deve ser utilizado link de via satélite com conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.
- 5.3.3. Deve ser fornecido 01 (um) link de internet via satélite com velocidade mínima de 100 Mbps de download. Não sendo permitida upgrade de velocidade ou incremento de link adicional neste item.
- 5.3.4. Deve suportar transporte de pacotes IPv4 e IPv6.
- 5.3.5. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 5.3.6. O link deve ser entregue e mantido sem restrições de volume de tráfego.
- 5.3.7. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 5.3.8. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 5.3.9. O link não poderá ter franquia de acesso que limite sua utilização.
- 5.3.10. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 5.3.11. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.
- 5.3.12. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 5.3.13. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 5.3.14. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 5.3.15. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 5.3.16. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 5.3.17. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 5.3.18. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem

tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

5.4. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

5.4.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:

- 5.4.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.
- 5.4.1.2. Ativação e testes de 01 Link de Internet Banda Larga , assegurando estabilidade e disponibilidade.
- 5.4.1.3. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

5.4.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:

- 5.4.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.
- 5.4.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.
- 5.4.2.3. Gerenciamento remoto e centralizado das políticas de segurança de endpoint.
- 5.4.2.4. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

6. LOTE 01 - ITEM 06 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 06

6.1. A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 06 deve ser implantada em unidades governamentais que necessitam de conectividade segura, proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, um link de internet banda larga, um link satélite, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

6.2. Caso a solução não implemente nativamente os recursos e funcionalidades exigidas será aceito composição com outras soluções desde que seja garantido e comprovado atendimento integral a todos os requisitos técnicos exigidos neste termo de referência e assegurando interoperabilidade plena entre os componentes que compõem a solução ofertada.

6.3. SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW

- 6.3.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.
- 6.3.2. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;
- 6.3.3. Poderá ser feita composição de soluções para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 6.3.4. Garantir que a solução disponibilize no(s) equipamento(s), acesso a gerência e monitoração, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
- 6.3.5. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.
- 6.3.6. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
- 6.3.7. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.
- 6.3.8. Deve suportar e estar licenciado para a criação de, ao menos, 10(dez) instâncias virtuais de firewall no mesmo hardware.
- 6.3.9. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 6.3.10. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

- 6.3.11. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 6.3.12. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 6.3.13. Deve possuir firewall com capacidade mínima de processamento de 6 (seis) Gbps.
- 6.3.14. Deve possuir IPS com capacidade mínima de processamento de 1 (um) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 6.3.15. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1,2 (um virgula dois) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 6.3.16. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 1,3 (um virgula três) Gbps.
- 6.3.17. Deve possuir VPN com capacidade de, pelo menos, 06 (seis) Gbps de tráfego IPSec.
- 6.3.18. Deve suportar 1.000.000 (um milhão) conexões simultâneas.
- 6.3.19. Deve suportar, pelo menos, 100.000 (cem mil) novas conexões por segundo.
- 6.3.20. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.
- 6.3.21. Deve suportar, pelo menos, 450 (quatrocentos e cinquenta) túneis de VPN Client-Site.
- 6.3.22. Deve possuir, pelo menos, 09 (nove) interfaces RJ45 1GE.
- 6.3.23. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 6.3.24. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 6.3.25. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.
- 6.3.26. FUNCIONALIDADES DE FIREWALL

- 6.3.26.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
- 6.3.26.2. Possuir suporte a sub-interfaces ethernet lógicas;
- 6.3.26.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
- 6.3.26.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
- 6.3.26.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 6.3.26.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 6.3.26.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 6.3.26.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 6.3.26.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 6.3.26.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 6.3.26.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 6.3.26.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 6.3.26.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 6.3.26.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 6.3.26.15. Deve suportar o encaminhamento de tráfego multicast.
- 6.3.26.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 6.3.26.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 6.3.26.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 6.3.26.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 6.3.26.20. Suportar OSPF gracefulrestart;
- 6.3.26.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 6.3.26.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 6.3.26.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall,

mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

- 6.3.26.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 6.3.26.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 6.3.26.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 6.3.26.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 6.3.26.28. Drop sem notificação do bloqueio ao usuário;
 - 6.3.26.29. Drop com notificação do bloqueio ao usuário;
 - 6.3.26.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 6.3.26.31. TCP-Reset para o cliente;
 - 6.3.26.32. TCP-Reset para o server ou para os dois lados da conexão.
- 6.3.26.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 6.3.26.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 6.3.26.35. Deve oferecer suporte ao protocolo SIP.
- 6.3.26.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 6.3.26.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 6.3.26.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 6.3.26.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 6.3.26.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 6.3.26.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.

- 6.3.26.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 6.3.26.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 6.3.26.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 6.3.26.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 6.3.26.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 6.3.26.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 6.3.26.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 6.3.26.49. Realizar Traffic Shaping para a solução de segurança
- 6.3.26.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 6.3.26.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 6.3.26.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 6.3.26.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 6.3.26.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 6.3.26.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 6.3.26.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 6.3.26.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de

uso das interfaces de rede;

- 6.3.26.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 6.3.26.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 6.3.26.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 6.3.26.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 6.3.26.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 6.3.26.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 6.3.26.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 6.3.26.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 6.3.26.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 6.3.26.67. Funcionar com tradução de porta (PAT);
- 6.3.26.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 6.3.26.69. Implementar e suportar NAT64 e NAT46;
- 6.3.26.70. Implementar NAT66
- 6.3.26.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 6.3.26.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 6.3.26.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 6.3.26.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 6.3.26.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores

abaixo:

6.3.26.75.1. Conectores SDN Privados:

- 6.3.26.75.1.1. Nutanix;
- 6.3.26.75.1.2. Kubernetes;
- 6.3.26.75.1.3. VMware ESXi;
- 6.3.26.75.1.4. OpenStack;

6.3.26.75.2. Conectores SDN Públicos;

- 6.3.26.75.2.1. Google Cloud Platform (GCP);
- 6.3.26.75.2.2. AWS;
- 6.3.26.75.2.3. Microsoft Azure;
- 6.3.26.75.2.4. Oracle Cloud Infrastructure (OCI);

6.3.26.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).

6.3.26.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;

6.3.26.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).

6.3.26.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.

6.3.26.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

6.3.27. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

6.3.27.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.

6.3.27.2. Deve permitir modificação de valores DSCP para o DiffServ.

6.3.27.3. Deve permitir priorização de tráfego e suportar ToS.

6.3.27.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.

6.3.27.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.

- 6.3.27.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 6.3.27.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 6.3.27.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 6.3.27.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
- 6.3.27.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.
- 6.3.28. **FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**
 - 6.3.28.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
 - 6.3.28.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
 - 6.3.28.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
 - 6.3.28.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
 - 6.3.28.5. Deve permitir a criação de categorias personalizadas.
 - 6.3.28.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
 - 6.3.28.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
 - 6.3.28.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
 - 6.3.28.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
 - 6.3.28.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
 - 6.3.28.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
 - 6.3.28.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
 - 6.3.28.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active

directory) e base de dados local;

- 6.3.28.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 6.3.28.15. Permitir a criação de categorias de URLs customizadas;
- 6.3.28.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 6.3.28.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 6.3.28.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 6.3.28.19. Permitir a customização de página de bloqueio;
- 6.3.28.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 6.3.28.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 6.3.28.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 6.3.28.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 6.3.28.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 6.3.28.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 6.3.28.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 6.3.28.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 6.3.28.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.

- 6.3.28.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 6.3.28.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 6.3.28.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 6.3.28.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 6.3.28.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 6.3.28.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 6.3.28.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 6.3.28.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 6.3.28.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 6.3.28.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 6.3.28.39. Deve possuir Proxy Explícito e Transparente.
- 6.3.28.40. Deve implementar roteamento WCCP e ICAP.
- 6.3.29. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)
 - 6.3.29.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
 - 6.3.29.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
 - 6.3.29.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
 - 6.3.29.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
 - 6.3.29.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
 - 6.3.29.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
 - 6.3.29.7. Deve permitir funcionar em modo transparente, sniffer e router.

- 6.3.29.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 6.3.29.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 6.3.29.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 6.3.29.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 6.3.29.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 6.3.29.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 6.3.29.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 6.3.29.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 6.3.29.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 6.3.29.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 6.3.29.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 6.3.29.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 6.3.29.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 6.3.29.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 6.3.29.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 6.3.29.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;

- 6.3.29.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 6.3.29.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 6.3.29.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 6.3.29.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 6.3.29.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 6.3.29.29. Identificar, alertar e bloquear comunicação com botnets;
- 6.3.29.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 6.3.29.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 6.3.29.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 6.3.29.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 6.3.29.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 6.3.29.35. Identificar nos eventos o país de onde partiu a ameaça;
- 6.3.29.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 6.3.29.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 6.3.29.38. Deve possuir alarmes na console de administração.
- 6.3.29.39. Deve possuir alertas via correio eletrônico.
- 6.3.29.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O

dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.

6.3.29.41. Deve ter a capacidade de resposta/logs ativa a ataques.

6.3.29.42. Incluir proteção contra ataques de negação de serviços (DoS);

6.3.29.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);

6.3.29.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

6.3.30. FUNCIONALIDADE DE VPN

6.3.30.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;

6.3.30.2. Suportar nativamente a criação de VPN IPsec utilizando 3DES;

6.3.30.3. Suportar nativamente a criação de VPN IPsec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;

6.3.30.4. Suportar nativamente a autenticação de VPN IPsec utilizando MD5 e SHA-1;

6.3.30.5. Suportar nativamente a criação de VPN IPsec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;

6.3.30.6. Suportar nativamente a criação de VPN IPsec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);

6.3.30.7. Suportar nativamente, para VPN IPsec, autenticação via certificado IKE PKI;

6.3.30.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPsec a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);

6.3.30.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;

6.3.30.10. Realizar atribuição de DNS nos clientes remotos de VPN;

6.3.30.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;

6.3.30.12. Suportar leitura e verificação de CRL (Certificate Revocation List);

6.3.30.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;

6.3.30.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;

6.3.30.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;

6.3.30.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.

6.3.30.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPsec estabelecidos.

6.3.31. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

6.3.31.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;

6.3.31.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;

6.3.31.3. Atualizar a base de assinaturas de aplicações automaticamente;

6.3.31.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.

6.3.31.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

6.3.31.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;

6.3.31.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;

6.3.31.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

6.3.31.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;

6.3.31.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;

6.3.31.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;

6.3.31.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;

6.3.31.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia

utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.

- 6.3.31.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 6.3.31.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 6.3.31.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 6.3.31.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 6.3.31.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 6.3.31.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 6.3.31.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 6.3.31.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 6.3.31.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 6.3.31.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 6.3.31.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 6.3.31.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 6.3.31.26. Deve permitir criação de padrões de aplicação manualmente.
- 6.3.31.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;

- 6.3.31.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 6.3.31.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 6.3.31.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent “encriptado” e aplicações VOIP que utilizam criptografia proprietária;

6.3.32. FUNCIONALIDADE DE SD-WAN

- 6.3.32.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
- 6.3.32.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.
- 6.3.32.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 6.3.32.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 6.3.32.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 6.3.32.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 6.3.32.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 6.3.32.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 6.3.32.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 6.3.32.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 6.3.32.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático

de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.

- 6.3.32.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 6.3.32.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 6.3.32.14. Passivo: uso do tráfego real para as medições;
- 6.3.32.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 6.3.32.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 6.3.32.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 6.3.32.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 6.3.32.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 6.3.32.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 6.3.32.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 6.3.32.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 6.3.32.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);

- 6.3.32.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 6.3.32.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 6.3.32.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 6.3.32.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 6.3.32.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 6.3.32.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

6.4. LINK DE CONECTIVIDADE BANDA LARGA EM DUPLA ABORDAGEM

- 6.4.1. Deve ser fornecidos dois links Banda Larga cada, sendo um com conectividade via satélite e outro com conectividade via fibra optica, para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.
- 6.4.2. Deve ser utilizados links de comunicação satélite e comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.
- 6.4.3. Deve ser fornecido 01 (um) link de internet com conectividade via fibra com velocidade mínima de 500 Mbps de download, e um link com conectividade via satélite com velocidade mínima de 100 Mbps.
- 6.4.4. O link de internet Banda Larga fornecido via fibra deverá disponibilizar endereçamento IP fixo em IPv6, válido e roteável na Internet, atribuído exclusivamente ao CONTRATANTE, não sendo permitido o uso de endereçamento dinâmico, NAT ou CGNAT para o tráfego IPv6.
- 6.4.5. Deve suportar transporte de pacotes IPv4 e IPv6.

- 6.4.6. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 6.4.7. O link deve ser entregue e mantido sem restrições de volume de tráfego.
- 6.4.8. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 6.4.9. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 6.4.10. O link não poderá ter franquia de acesso que limite sua utilização.
- 6.4.11. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 6.4.12. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.
- 6.4.13. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 6.4.14. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 6.4.15. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 6.4.16. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 6.4.17. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 6.4.18. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 6.4.19. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 6.4.20. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

6.5. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

- 6.5.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:
 - 6.5.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo

conectividade segura e controle de tráfego.

6.5.1.2. Ativação e testes de 02 Links de Internet Banda Larga, assegurando estabilidade e disponibilidade.

6.5.1.3. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

6.5.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:

6.5.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.

6.5.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.

6.5.2.3. Gerenciamento remoto e centralizado das políticas de segurança de endpoint.

6.5.2.4. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

7. LOTE 01 - ITEM 07 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 07

7.1. A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 07 deve ser implantada em unidades governamentais que necessitam de conectividade segura, com link de internet banda larga, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

7.2. Caso a solução não implemente nativamente os recursos e funcionalidades exigidas será aceito composição com outras soluções desde que seja garantido e comprovado atendimento integral a todos os requisitos técnicos exigidos neste termo de referência e assegurando interoperabilidade plena entre os componentes que compõem a solução ofertada.

7.3. LINK DE CONECTIVIDADE BANDA LARGA

7.3.1. O link de 500 Mbps Banda Larga serão fornecidos para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.

7.3.2. Deve ser utilizado link de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.

7.3.3. Deve ser fornecido 01 (um) link de internet com velocidade mínima de 500 Mbps de download.

7.3.4. O link de internet Banda Larga fornecido deverá disponibilizar endereçamento IP fixo em

IPv6, válido e roteável na Internet, atribuído exclusivamente ao CONTRATANTE, não sendo permitido o uso de endereçamento dinâmico, NAT ou CGNAT para o tráfego IPv6.

- 7.3.5. Deve suportar transporte de pacotes IPv4 e IPv6.
- 7.3.6. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 7.3.7. O link deve ser entregue e mantido sem restrições de volume de tráfego.
- 7.3.8. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 7.3.9. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 7.3.10. O link não poderá ter franquia de acesso que limite sua utilização.
- 7.3.11. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 7.3.12. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.
- 7.3.13. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 7.3.14. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 7.3.15. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 7.3.16. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 7.3.17. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 7.3.18. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 7.3.19. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 7.3.20. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

7.4. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

7.4.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:

7.4.1.1. Ativação e testes de 01 Link de Internet Banda Larga, assegurando estabilidade e disponibilidade.

7.4.1.2. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

7.4.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle.

8. LOTE 01 - ITEM 08 - SOLUÇÃO DE CONECTIVIDADE SEGURA -TIPO 08

8.1. A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 08 deve ser implantada em unidades governamentais que necessitam de conectividade segura, com dois links de internet banda larga, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

8.2. LINK DE CONECTIVIDADE BANDA LARGA EM DUPLA ABORDAGEM

8.2.1. Links de conectividade adicional, sendo 02 (dois) links de 500 Mbps Banda Larga serão fornecidos para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.

8.2.2. Deverão ser utilizados links de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.

8.2.3. Deve ser fornecido 02 (dois) link de internet adicional, com velocidade mínima de 500 Mbps de download, garantindo redundância e disponibilidade contínua.

8.2.4. Os circuitos de internet terrestre em cada unidade deverão ser entregues cada um por uma operadora ou provedor exclusivo.

8.2.5. Os links devem ser estabelecidos por caminhos completamente distintos, não devendo haver nenhum ponto de falha comum entre os dois links de comunicação.

8.2.6. Os circuitos de internet terrestre em cada unidade deverão ser entregues cada um por uma operadora ou provedor exclusivo.

8.2.7. Os links devem ser estabelecidos por caminhos completamente distintos, não devendo haver nenhum ponto de falha comum entre os dois links de comunicação.

8.2.8. Os links de internet Banda Larga fornecidos deverão disponibilizar endereçamento IP fixo em IPv6, válido e roteável na Internet, atribuído exclusivamente ao CONTRATANTE, não sendo

permitido o uso de endereçamento dinâmico, NAT ou CGNAT para o tráfego IPv6.

8.2.9. Deve suportar transporte de pacotes IPv4 e IPv6.

8.2.10. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.

8.2.11. O link deve ser entregue e mantido sem restrições de volume de tráfego.

8.2.12. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.

8.2.13. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.

8.2.14. O link não poderá ter franquia de acesso que limite sua utilização.

8.2.15. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.

8.2.16. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.

8.2.17. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.

8.2.18. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.

8.2.19. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.

8.2.20. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.

8.2.21. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.

8.2.22. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.

8.2.23. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.

8.2.24. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

8.3. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

8.3.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local,

incluindo:

- 8.3.1.1. Ativação e testes de 02 Links de Internet Banda Larga , assegurando estabilidade e disponibilidade.
- 8.3.1.2. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.
- 8.3.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle.

9. LOTE 01 - ITEM 09 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 09

- 9.1. A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 09 deve ser implantada em unidades governamentais que necessitam de conectividade segura, com link de internet banda larga, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:
- 9.2. Caso a solução não implemente nativamente os recursos e funcionalidades exigidas será aceito composição com outras soluções desde que seja garantido e comprovado atendimento integral a todos os requisitos técnicos exigidos neste termo de referência e assegurando interoperabilidade plena entre os componentes que compõem a solução ofertada.

9.3. LINK DE CONECTIVIDADE BANDA LARGA

- 9.3.1. O link de 1 Gbps Banda Larga serão fornecidos para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.
- 9.3.2. Deve ser utilizado link de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.
- 9.3.3. Deve ser fornecido 01 (um) link de internet com velocidade mínima de 1 Gbps de download.
- 9.3.4. Para os locais em que não houver viabilidade técnica da CONTRATADA disponibilizar um link de internet com capacidade de 1 (um) Gbps, será admitida, mediante justificativa técnica, a entrega de 2 (dois) links distintos com capacidade mínima de 500 (quinhentos) Mbps cada, de forma a garantir a capacidade total equivalente.
- 9.3.5. O link de internet Banda Larga fornecido deverá disponibilizar endereçamento IP fixo em IPv6, válido e roteável na Internet, atribuído exclusivamente ao CONTRATANTE, não sendo permitido o uso de endereçamento dinâmico, NAT ou CGNAT para o tráfego IPv6.
- 9.3.6. Deve suportar transporte de pacotes IPv4 e IPv6.

- 9.3.7. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 9.3.8. O link deve ser entregue e mantido sem restrições de volume de tráfego.
- 9.3.9. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 9.3.10. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 9.3.11. O link não poderá ter franquia de acesso que limite sua utilização.
- 9.3.12. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 9.3.13. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.
- 9.3.14. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 9.3.15. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 9.3.16. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 9.3.17. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 9.3.18. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 9.3.19. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 9.3.20. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 9.3.21. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

9.4.IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

- 9.4.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:
- 9.4.1.1. Ativação e testes de 01 Link de Internet Banda Larga , assegurando estabilidade e

disponibilidade.

9.4.1.2. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

9.4.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle.

10. LOTE 01 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 10

10.1.A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 10 deve ser implantada em unidades governamentais que necessitam de conectividade segura, com dois links de internet banda larga, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

10.2. LINK DE CONECTIVIDADE BANDA LARGA EM DUPLA ABORDAGEM

10.2.1. Links de conectividade adicional, sendo 02 (dois) links de 1 Gbps Banda Larga serão fornecidos para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.

10.2.2. Deverão ser utilizados links de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.

10.2.3. Deve ser fornecido 02 (dois) link de internet adicional, com velocidade mínima de 1 Gbps de download, garantindo redundância e disponibilidade contínua.

10.2.4. Para os locais em que não houver viabilidade técnica da CONTRATADA disponibilizar um link de internet com capacidade de 1 (um) Gbps, será admitida, mediante justificativa técnica, a entrega de 2 (dois) links distintos com capacidade mínima de 500 (quinhentos) Mbps cada, de forma a garantir a capacidade total equivalente.

10.2.5. Os circuitos de internet terrestre em cada unidade deverão ser entregues cada um por uma operadora ou provedor exclusivo.

10.2.6. Os links devem ser estabelecidos por caminhos completamente distintos, não devendo haver nenhum ponto de falha comum entre os dois links de comunicação.

10.2.7. Os links de internet Banda Larga fornecidos deverão disponibilizar endereçamento IP fixo em IPv6, válido e roteável na Internet, atribuído exclusivamente ao CONTRATANTE, não sendo permitido o uso de endereçamento dinâmico, NAT ou CGNAT para o tráfego IPv6.

10.2.8. Deve suportar transporte de pacotes IPv4 e IPv6.

- 10.2.9. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 10.2.10. O link deve ser entregue e mantido sem restrições de volume de tráfego.
- 10.2.11. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 10.2.12. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 10.2.13. O link não poderá ter franquia de acesso que limite sua utilização.
- 10.2.14. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 10.2.15. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.
- 10.2.16. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 10.2.17. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 10.2.18. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 10.2.19. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 10.2.20. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 10.2.21. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 10.2.22. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 10.2.23. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

10.3. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

- 10.3.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:
 - 10.3.1.1. Ativação e testes de 02 Links de Internet Banda Larga , assegurando estabilidade e

disponibilidade.

10.3.1.2. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

10.3.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle.

11. LOTE 01 - ITEM 11 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 11

11.1.A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 11 deve ser implantada em unidades governamentais que necessitam de conectividade segura, com um link satélite de internet banda larga, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

11.2. LINK DE CONECTIVIDADE SATÉLITE

11.2.1. Links de conectividade satélite com 100 Mbps Banda Larga serão fornecidos para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.

11.2.2. Deverão ser utilizados links de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.

11.2.3. Deve ser fornecido 01 (um) link de internet via satélite, com velocidade mínima de 100 Mbps de download, garantindo redundância e disponibilidade contínua.

11.2.4. Deve suportar transporte de pacotes IPv4 e IPv6.

11.2.5. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.

11.2.6. O link deve ser entregue e mantido sem restrições de volume de tráfego.

11.2.7. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.

11.2.8. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.

11.2.9. O link não poderá ter franquia de acesso que limite sua utilização.

11.2.10. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.

11.2.11. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.

- 11.2.12. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 11.2.13. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 11.2.14. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 11.2.15. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 11.2.16. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 11.2.17. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 11.2.18. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

11.3.IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

- 11.3.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:
 - 11.3.1.1. Ativação e testes de 01 Links de Internet assegurando estabilidade e disponibilidade.
 - 11.3.1.2. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.
- 11.3.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle.

12.LOTE 01 - ITEM 12 - SOLUÇÃO DE CONECTIVIDADE SEGURA -TIPO 12

- 12.1.A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 12 deve ser implantada em unidades governamentais que necessitam de conectividade segura, com um link de internet banda larga, um link satélite, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:
- 12.2.LINK DE CONECTIVIDADE BANDA LARGA EM DUPLA ABORDAGEM
 - 12.2.1. Deve ser fornecidos dois links Banda Larga cada, sendo um com conectividade via

satélite e outro com conectividade via fibra óptica, para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.

- 12.2.2. Deve ser utilizados links de comunicação satélite e comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.
- 12.2.3. Deve ser fornecido 01 (um) link de internet com conectividade via fibra com velocidade mínima de 500 Mbps de download, e um link com conectividade via satélite com velocidade mínima de 100 Mbps.
- 12.2.4. O link de internet Banda Larga fornecido via fibra deverá disponibilizar endereçamento IP fixo em IPv6, válido e roteável na Internet, atribuído exclusivamente ao CONTRATANTE, não sendo permitido o uso de endereçamento dinâmico, NAT ou CGNAT para o tráfego IPv6.
- 12.2.5. Deve suportar transporte de pacotes IPv4 e IPv6.
- 12.2.6. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 12.2.7. O link deve ser entregue e mantido sem restrições de volume de tráfego.
- 12.2.8. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 12.2.9. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 12.2.10. O link não poderá ter franquia de acesso que limite sua utilização.
- 12.2.11. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 12.2.12. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.
- 12.2.13. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 12.2.14. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 12.2.15. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 12.2.16. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 12.2.17. A Contratada será responsável pela instalação e ativação da infraestrutura necessária

nos locais indicados pela Contratante.

12.2.18. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.

12.2.19. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.

12.2.20. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

12.3. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

12.3.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:

12.3.1.1. Ativação e testes de 02 Links de Internet Banda Larga, assegurando estabilidade e disponibilidade.

12.3.1.2. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

12.3.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle.

13. LOTE 01 - ITEM 13 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 13

13.1.A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 13 deve ser implantada em unidades governamentais que necessitam de conectividade segura, proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

13.2. SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW

13.2.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.

13.2.2. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance físico), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma

- solução, ou seja, hardware e software devem ser integrados em um único equipamento;
- 13.2.3. Poderá ser feita composição de soluções para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 13.2.4. A solução deve permitir acesso a gerência e monitoramento, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
- 13.2.5. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.
- 13.2.6. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
- 13.2.7. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.
- 13.2.8. Deve suportar e estar licenciado para a criação de, ao menos, 10 (dez) instâncias virtuais de firewall no mesmo hardware.
- 13.2.9. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 13.2.10. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 13.2.11. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 13.2.12. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 13.2.13. Deve possuir firewall com capacidade mínima de processamento de 6 (seis) Gbps.
- 13.2.14. Deve possuir IPS com capacidade mínima de processamento de 1 (um) Gbps. Para

efeitos de comprovação pode também ser considerado o throughput de Threat Protection.

- 13.2.15. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1,2 (um virgula dois) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 13.2.16. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 1,3 (um virgula três) Gbps.
- 13.2.17. Deve possuir VPN com capacidade de, pelo menos, 06 (seis) Gbps de tráfego IPSec.
- 13.2.18. Deve suportar 1.000.000 (um milhão) conexões simultâneas.
- 13.2.19. Deve suportar, pelo menos, 100.000 (cem mil) novas conexões por segundo.
- 13.2.20. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.
- 13.2.21. Deve suportar, pelo menos, 450 (quatrocentos e cinquenta) túneis de VPN Client-Site.
- 13.2.22. Deve possuir, pelo menos, 09 (nove) interfaces RJ45 1GE.
- 13.2.23. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 13.2.24. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 13.2.25. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.
- 13.2.26. FUNCIONALIDADES DE FIREWALL
 - 13.2.26.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
 - 13.2.26.2. Possuir suporte a sub-interfaces ethernet lógicas;
 - 13.2.26.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
 - 13.2.26.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.

- 13.2.26.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 13.2.26.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 13.2.26.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 13.2.26.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 13.2.26.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 13.2.26.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 13.2.26.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 13.2.26.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 13.2.26.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 13.2.26.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 13.2.26.15. Deve suportar o encaminhamento de tráfego multicast.
- 13.2.26.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 13.2.26.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 13.2.26.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 13.2.26.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 13.2.26.20. Suportar OSPF gracefulrestart;
- 13.2.26.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 13.2.26.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 13.2.26.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer

(monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

- 13.2.26.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 13.2.26.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 13.2.26.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 13.2.26.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 13.2.26.28. Drop sem notificação do bloqueio ao usuário;
 - 13.2.26.29. Drop com notificação do bloqueio ao usuário;
 - 13.2.26.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 13.2.26.31. TCP-Reset para o cliente;
 - 13.2.26.32. TCP-Reset para o server ou para os dois lados da conexão.
 - 13.2.26.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 13.2.26.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 13.2.26.35. Deve oferecer suporte ao protocolo SIP.
- 13.2.26.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 13.2.26.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 13.2.26.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 13.2.26.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 13.2.26.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 13.2.26.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.

- 13.2.26.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 13.2.26.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 13.2.26.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 13.2.26.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 13.2.26.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 13.2.26.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 13.2.26.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 13.2.26.49. Realizar Traffic Shaping para a solução de segurança
- 13.2.26.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 13.2.26.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 13.2.26.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 13.2.26.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 13.2.26.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 13.2.26.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 13.2.26.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 13.2.26.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e

estatísticas de uso das interfaces de rede;

- 13.2.26.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 13.2.26.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 13.2.26.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 13.2.26.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 13.2.26.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 13.2.26.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 13.2.26.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 13.2.26.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 13.2.26.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 13.2.26.67. Funcionar com tradução de porta (PAT);
- 13.2.26.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 13.2.26.69. Implementar e suportar NAT64 e NAT46;
- 13.2.26.70. Implementar NAT66
- 13.2.26.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 13.2.26.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 13.2.26.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 13.2.26.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 13.2.26.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados

em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:

13.2.26.75.1. Conectores SDN Privados:

- 13.2.26.75.1.1. Nutanix;
- 13.2.26.75.1.2. Kubernetes;
- 13.2.26.75.1.3. VMware ESXi;
- 13.2.26.75.1.4. OpenStack;

13.2.26.75.2. Conectores SDN Públicos;

- 13.2.26.75.2.1. Google Cloud Platform (GCP);
- 13.2.26.75.2.2. AWS;
- 13.2.26.75.2.3. Microsoft Azure;
- 13.2.26.75.2.4. Oracle Cloud Infrastructure (OCI);

13.2.26.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).

13.2.26.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;

13.2.26.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).

13.2.26.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.

13.2.26.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

13.2.27. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

13.2.27.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.

13.2.27.2. Deve permitir modificação de valores DSCP para o DiffServ.

13.2.27.3. Deve permitir priorização de tráfego e suportar ToS.

13.2.27.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.

13.2.27.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active

Directory, reconhecendo grupos de usuários cadastrados.

13.2.27.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.

13.2.27.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.

13.2.27.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.

13.2.27.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.

13.2.27.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

13.2.28. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

13.2.28.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.

13.2.28.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.

13.2.28.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.

13.2.28.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

13.2.28.5. Deve permitir a criação de categorias personalizadas.

13.2.28.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.

13.2.28.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.

13.2.28.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.

13.2.28.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.

13.2.28.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;

13.2.28.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

13.2.28.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

- 13.2.28.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 13.2.28.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 13.2.28.15. Permitir a criação de categorias de URLs customizadas;
- 13.2.28.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 13.2.28.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 13.2.28.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 13.2.28.19. Permitir a customização de página de bloqueio;
- 13.2.28.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 13.2.28.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 13.2.28.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 13.2.28.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 13.2.28.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 13.2.28.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 13.2.28.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 13.2.28.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;

- 13.2.28.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 13.2.28.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 13.2.28.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 13.2.28.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 13.2.28.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 13.2.28.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 13.2.28.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 13.2.28.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 13.2.28.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 13.2.28.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 13.2.28.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 13.2.28.39. Deve possuir Proxy Explícito e Transparente.
- 13.2.28.40. Deve implementar roteamento WCCP e ICAP.
- 13.2.29. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)
 - 13.2.29.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
 - 13.2.29.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
 - 13.2.29.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
 - 13.2.29.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
 - 13.2.29.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para

- ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 13.2.29.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 13.2.29.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 13.2.29.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 13.2.29.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 13.2.29.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 13.2.29.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 13.2.29.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 13.2.29.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 13.2.29.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 13.2.29.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 13.2.29.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 13.2.29.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 13.2.29.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 13.2.29.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 13.2.29.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 13.2.29.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message

Protocol).

- 13.2.29.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 13.2.29.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 13.2.29.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 13.2.29.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 13.2.29.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 13.2.29.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 13.2.29.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 13.2.29.29. Identificar, alertar e bloquear comunicação com botnets;
- 13.2.29.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 13.2.29.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 13.2.29.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 13.2.29.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 13.2.29.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

- 13.2.29.35. Identificar nos eventos o país de onde partiu a ameaça;
- 13.2.29.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 13.2.29.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 13.2.29.38. Deve possuir alarmes na console de administração.
- 13.2.29.39. Deve possuir alertas via correio eletrônico.
- 13.2.29.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 13.2.29.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 13.2.29.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 13.2.29.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 13.2.29.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;
- 13.2.30. FUNCIONALIDADE DE VPN
 - 13.2.30.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
 - 13.2.30.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
 - 13.2.30.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
 - 13.2.30.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
 - 13.2.30.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
 - 13.2.30.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
 - 13.2.30.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
 - 13.2.30.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
 - 13.2.30.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;

- 13.2.30.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 13.2.30.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 13.2.30.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 13.2.30.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 13.2.30.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 13.2.30.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 13.2.30.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 13.2.30.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSec estabelecidos.
- 13.2.31. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
 - 13.2.31.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
 - 13.2.31.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
 - 13.2.31.3. Atualizar a base de assinaturas de aplicações automaticamente;
 - 13.2.31.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
 - 13.2.31.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
 - 13.2.31.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
 - 13.2.31.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de

- ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 13.2.31.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 13.2.31.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 13.2.31.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 13.2.31.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 13.2.31.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 13.2.31.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 13.2.31.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 13.2.31.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 13.2.31.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 13.2.31.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 13.2.31.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 13.2.31.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 13.2.31.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 13.2.31.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo

de usuários do Microsoft Active Directory.

- 13.2.31.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 13.2.31.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 13.2.31.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 13.2.31.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 13.2.31.26. Deve permitir criação de padrões de aplicação manualmente.
- 13.2.31.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 13.2.31.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 13.2.31.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 13.2.31.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;
- 13.2.32. FUNCIONALIDADE DE SD-WAN
 - 13.2.32.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
 - 13.2.32.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.
 - 13.2.32.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
 - 13.2.32.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
 - 13.2.32.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
 - 13.2.32.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de

inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;

- 13.2.32.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 13.2.32.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/range de IPs de destino;
- 13.2.32.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 13.2.32.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 13.2.32.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 13.2.32.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 13.2.32.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 13.2.32.14. Passivo: uso do tráfego real para as medições;
- 13.2.32.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 13.2.32.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 13.2.32.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 13.2.32.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 13.2.32.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet

Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;

- 13.2.32.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 13.2.32.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 13.2.32.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 13.2.32.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 13.2.32.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 13.2.32.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 13.2.32.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 13.2.32.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 13.2.32.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 13.2.32.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

13.3. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

13.3.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:

13.3.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.

13.3.1.2. Ativação e testes dos links existentes, assegurando estabilidade e disponibilidade.

13.3.1.3. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

13.3.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:

13.3.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.

13.3.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.

13.3.2.3. Gerenciamento remoto e centralizado das políticas de segurança de endpoint.

13.3.2.4. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

14. LOTE 01 - ITEM 14 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 14

14.1.A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 14 deve ser implantada em unidades governamentais que necessitam de conectividade segura, proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

14.2. SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW

14.2.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.

14.2.2. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;

- 14.2.3. Poderá ser feita composição de soluções para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 14.2.4. Garantir que a solução disponibilize no(s) equipamento(s), acesso a gerência e monitoração, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
- 14.2.5. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.
- 14.2.6. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
- 14.2.7. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.
- 14.2.8. Deve suportar e estar licenciado para a criação de, ao menos 10(dez) instâncias virtuais de firewall no mesmo hardware.
- 14.2.9. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 14.2.10. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 14.2.11. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 14.2.12. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 14.2.13. Deve possuir firewall com capacidade mínima de processamento de 26 (vinte e seis) Gbps.

- 14.2.14. Deve possuir IPS com capacidade mínima de processamento de 5 (cinco) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 14.2.15. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 2,5 (dois vírgula cinco) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 14.2.16. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 3 (três) Gbps.
- 14.2.17. Deve possuir VPN com capacidade de, pelo menos, 33 (trinta e três) Gbps de tráfego IPSec.
- 14.2.18. Deve suportar 3.000.000 (três milhões) conexões simultâneas.
- 14.2.19. Deve suportar, pelo menos, 135.000 (cento e trinta e cinco mil) novas conexões por segundo.
- 14.2.20. Deve suportar, pelo menos, 1800 (mil e oitocentos) túneis de VPN Site-Site.
- 14.2.21. Deve suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site.
- 14.2.22. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE.
- 14.2.23. Deve possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE.
- 14.2.24. Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.
- 14.2.25. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 14.2.26. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 14.2.27. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.
- 14.2.28. FUNCIONALIDADES DE FIREWALL
- 14.2.28.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
- 14.2.28.2. Possuir suporte a sub-interfaces ethernet lógicas;

- 14.2.28.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
- 14.2.28.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
- 14.2.28.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 14.2.28.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 14.2.28.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 14.2.28.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 14.2.28.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 14.2.28.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 14.2.28.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 14.2.28.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 14.2.28.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 14.2.28.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 14.2.28.15. Deve suportar o encaminhamento de tráfego multicast.
- 14.2.28.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 14.2.28.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 14.2.28.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 14.2.28.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 14.2.28.20. Suportar OSPF gracefulrestart;
- 14.2.28.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 14.2.28.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based

Routing).

- 14.2.28.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 14.2.28.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 14.2.28.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 14.2.28.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 14.2.28.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 14.2.28.28. Drop sem notificação do bloqueio ao usuário;
 - 14.2.28.29. Drop com notificação do bloqueio ao usuário;
 - 14.2.28.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 14.2.28.31. TCP-Reset para o cliente;
 - 14.2.28.32. TCP-Reset para o server ou para os dois lados da conexão.
- 14.2.28.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 14.2.28.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 14.2.28.35. Deve oferecer suporte ao protocolo SIP.
- 14.2.28.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 14.2.28.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 14.2.28.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 14.2.28.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 14.2.28.40. Deve permitir a criação de regras com base em usuário, grupo de usuários,

endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.

- 14.2.28.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 14.2.28.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 14.2.28.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 14.2.28.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 14.2.28.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 14.2.28.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 14.2.28.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 14.2.28.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 14.2.28.49. Realizar Traffic Shaping para a solução de segurança
- 14.2.28.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 14.2.28.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 14.2.28.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 14.2.28.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 14.2.28.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 14.2.28.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 14.2.28.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory

e RADIUS.

- 14.2.28.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 14.2.28.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 14.2.28.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 14.2.28.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 14.2.28.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 14.2.28.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 14.2.28.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 14.2.28.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 14.2.28.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 14.2.28.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 14.2.28.67. Funcionar com tradução de porta (PAT);
- 14.2.28.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 14.2.28.69. Implementar e suportar NAT64 e NAT46;
- 14.2.28.70. Implementar NAT66
- 14.2.28.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 14.2.28.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 14.2.28.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 14.2.28.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 14.2.28.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas

e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:

14.2.28.75.1. Conectores SDN Privados:

- 14.2.28.75.1.1. Nutanix;
- 14.2.28.75.1.2. Kubernetes;
- 14.2.28.75.1.3. VMware ESXi;
- 14.2.28.75.1.4. OpenStack;

14.2.28.75.2. Conectores SDN Públicos;

- 14.2.28.75.2.1. Google Cloud Platform (GCP);
- 14.2.28.75.2.2. AWS;
- 14.2.28.75.2.3. Microsoft Azure;
- 14.2.28.75.2.4. Oracle Cloud Infrastructure (OCI);

14.2.28.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).

14.2.28.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;

14.2.28.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).

14.2.28.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.

14.2.28.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

14.2.29. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

14.2.29.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.

14.2.29.2. Deve permitir modificação de valores DSCP para o DiffServ.

14.2.29.3. Deve permitir priorização de tráfego e suportar ToS.

- 14.2.29.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
- 14.2.29.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 14.2.29.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 14.2.29.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 14.2.29.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 14.2.29.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
- 14.2.29.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.
- 14.2.30. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB
 - 14.2.30.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
 - 14.2.30.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
 - 14.2.30.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
 - 14.2.30.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
 - 14.2.30.5. Deve permitir a criação de categorias personalizadas.
 - 14.2.30.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
 - 14.2.30.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
 - 14.2.30.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
 - 14.2.30.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
 - 14.2.30.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
 - 14.2.30.11. Permitir especificar política por tempo, ou seja, a definição de regras para um

determinado horário ou período (dia, mês, ano, dia da semana e hora);

- 14.2.30.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 14.2.30.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 14.2.30.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 14.2.30.15. Permitir a criação de categorias de URLs customizadas;
- 14.2.30.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 14.2.30.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 14.2.30.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 14.2.30.19. Permitir a customização de página de bloqueio;
- 14.2.30.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 14.2.30.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 14.2.30.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 14.2.30.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 14.2.30.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 14.2.30.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

- 14.2.30.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 14.2.30.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 14.2.30.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 14.2.30.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 14.2.30.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 14.2.30.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 14.2.30.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 14.2.30.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 14.2.30.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 14.2.30.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 14.2.30.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 14.2.30.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 14.2.30.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 14.2.30.39. Deve possuir Proxy Explícito e Transparente.
- 14.2.30.40. Deve implementar roteamento WCCP e ICAP.
- 14.2.31. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)
 - 14.2.31.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
 - 14.2.31.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
 - 14.2.31.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

- 14.2.31.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 14.2.31.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 14.2.31.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 14.2.31.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 14.2.31.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 14.2.31.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 14.2.31.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 14.2.31.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 14.2.31.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 14.2.31.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 14.2.31.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 14.2.31.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 14.2.31.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 14.2.31.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 14.2.31.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).

- 14.2.31.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 14.2.31.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 14.2.31.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 14.2.31.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 14.2.31.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 14.2.31.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 14.2.31.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 14.2.31.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 14.2.31.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 14.2.31.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 14.2.31.29. Identificar, alertar e bloquear comunicação com botnets;
- 14.2.31.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 14.2.31.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 14.2.31.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 14.2.31.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos

positivos;

- 14.2.31.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
 - 14.2.31.35. Identificar nos eventos o país de onde partiu a ameaça;
 - 14.2.31.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
 - 14.2.31.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
 - 14.2.31.38. Deve possuir alarmes na console de administração.
 - 14.2.31.39. Deve possuir alertas via correio eletrônico.
 - 14.2.31.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
 - 14.2.31.41. Deve ter a capacidade de resposta/logs ativa a ataques.
 - 14.2.31.42. Incluir proteção contra ataques de negação de serviços (DoS);
 - 14.2.31.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
 - 14.2.31.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;
- 14.2.32. FUNCIONALIDADE DE VPN
- 14.2.32.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
 - 14.2.32.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
 - 14.2.32.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
 - 14.2.32.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
 - 14.2.32.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
 - 14.2.32.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
 - 14.2.32.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
 - 14.2.32.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de resolução de problemas

(troubleshooting);

14.2.32.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;

14.2.32.10. Realizar atribuição de DNS nos clientes remotos de VPN;

14.2.32.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;

14.2.32.12. Suportar leitura e verificação de CRL (Certificate Revocation List);

14.2.32.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;

14.2.32.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;

14.2.32.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;

14.2.32.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.

14.2.32.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSec estabelecidos.

14.2.33. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

14.2.33.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;

14.2.33.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;

14.2.33.3. Atualizar a base de assinaturas de aplicações automaticamente;

14.2.33.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.

14.2.33.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

14.2.33.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no

mínimo, checagem de assinaturas e decodificação de protocolos;

- 14.2.33.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 14.2.33.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 14.2.33.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 14.2.33.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 14.2.33.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 14.2.33.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 14.2.33.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 14.2.33.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 14.2.33.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 14.2.33.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 14.2.33.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 14.2.33.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 14.2.33.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.

- 14.2.33.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 14.2.33.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 14.2.33.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 14.2.33.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 14.2.33.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 14.2.33.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 14.2.33.26. Deve permitir criação de padrões de aplicação manualmente.
- 14.2.33.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 14.2.33.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 14.2.33.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 14.2.33.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;
- 14.2.34. FUNCIONALIDADE DE SD-WAN
 - 14.2.34.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
 - 14.2.34.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.
 - 14.2.34.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
 - 14.2.34.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

- 14.2.34.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 14.2.34.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 14.2.34.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 14.2.34.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 14.2.34.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 14.2.34.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 14.2.34.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 14.2.34.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 14.2.34.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 14.2.34.14. Passivo: uso do tráfego real para as medições;
- 14.2.34.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 14.2.34.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 14.2.34.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 14.2.34.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de

pacote de dados;

- 14.2.34.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 14.2.34.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 14.2.34.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 14.2.34.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 14.2.34.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 14.2.34.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 14.2.34.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 14.2.34.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 14.2.34.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 14.2.34.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 14.2.34.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre

um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

14.3. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

14.3.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:

14.3.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.

14.3.1.2. Ativação e testes dos links de banda larga existentes, assegurando estabilidade e disponibilidade.

14.3.1.3. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

14.3.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:

14.3.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.

14.3.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.

14.3.2.3. Gerenciamento remoto e centralizado das políticas de segurança de endpoint.

14.3.2.4. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

15. LOTE 01 - ITEM 15 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 15

15.1.A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 15 deve ser implantada em unidades governamentais que necessitam de conectividade segura, proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, três links de internet banda larga, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

15.2. SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW

15.2.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.

- 15.2.2. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;
- 15.2.3. Poderá ser feita composição de soluções para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 15.2.4. Garantir que a solução disponibilize no(s) equipamento(s), acesso a gerência e monitoração, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
- 15.2.5. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.
- 15.2.6. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
- 15.2.7. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.
- 15.2.8. Deve suportar e estar licenciado para a criação de, ao menos 10(dez) instâncias virtuais de firewall no mesmo hardware.
- 15.2.9. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 15.2.10. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 15.2.11. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição,

remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

- 15.2.12. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 15.2.13. Deve possuir firewall com capacidade mínima de processamento de 26 (vinte e seis) Gbps.
- 15.2.14. Deve possuir IPS com capacidade mínima de processamento de 5 (cinco) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 15.2.15. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 2,5 (dois vírgula cinco) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 15.2.16. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 3 (três) Gbps.
- 15.2.17. Deve possuir VPN com capacidade de, pelo menos, 33 (trinta e três) Gbps de tráfego IPSec.
- 15.2.18. Deve suportar 3.000.000 (três milhões) conexões simultâneas.
- 15.2.19. Deve suportar, pelo menos, 135.000 (cento e trinta e cinco mil) novas conexões por segundo.
- 15.2.20. Deve suportar, pelo menos, 1800 (mil e oitocentos) túneis de VPN Site-Site.
- 15.2.21. Deve suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site.
- 15.2.22. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE.
- 15.2.23. Deve possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE.
- 15.2.24. Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.
- 15.2.25. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 15.2.26. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 15.2.27. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a

URL oficial do fabricante, em português do Brasil ou em inglês.

15.2.28. FUNCIONALIDADES DE FIREWALL

- 15.2.28.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
- 15.2.28.2. Possuir suporte a sub-interfaces ethernet lógicas;
- 15.2.28.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
- 15.2.28.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
- 15.2.28.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 15.2.28.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 15.2.28.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 15.2.28.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 15.2.28.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 15.2.28.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 15.2.28.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 15.2.28.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 15.2.28.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 15.2.28.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 15.2.28.15. Deve suportar o encaminhamento de tráfego multicast.
- 15.2.28.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 15.2.28.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 15.2.28.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 15.2.28.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);

- 15.2.28.20. Suportar OSPF gracefulrestart;
- 15.2.28.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 15.2.28.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 15.2.28.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 15.2.28.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 15.2.28.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 15.2.28.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 15.2.28.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 15.2.28.28. Drop sem notificação do bloqueio ao usuário;
 - 15.2.28.29. Drop com notificação do bloqueio ao usuário;
 - 15.2.28.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 15.2.28.31. TCP-Reset para o cliente;
 - 15.2.28.32. TCP-Reset para o server ou para os dois lados da conexão.
- 15.2.28.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 15.2.28.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 15.2.28.35. Deve oferecer suporte ao protocolo SIP.
- 15.2.28.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 15.2.28.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.

- 15.2.28.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 15.2.28.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 15.2.28.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 15.2.28.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 15.2.28.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 15.2.28.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 15.2.28.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 15.2.28.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 15.2.28.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 15.2.28.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 15.2.28.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 15.2.28.49. Realizar Traffic Shaping para a solução de segurança
- 15.2.28.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 15.2.28.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 15.2.28.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 15.2.28.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);

- 15.2.28.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 15.2.28.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 15.2.28.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 15.2.28.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 15.2.28.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 15.2.28.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 15.2.28.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 15.2.28.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 15.2.28.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 15.2.28.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 15.2.28.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 15.2.28.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 15.2.28.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 15.2.28.67. Funcionar com tradução de porta (PAT);
- 15.2.28.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 15.2.28.69. Implementar e suportar NAT64 e NAT46;
- 15.2.28.70. Implementar NAT66
- 15.2.28.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 15.2.28.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 15.2.28.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem

interrupção das conexões.

15.2.28.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.

15.2.28.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:

15.2.28.75.1. Conectores SDN Privados:

- 15.2.28.75.1.1. Nutanix;
- 15.2.28.75.1.2. Kubernetes;
- 15.2.28.75.1.3. VMware ESXi;
- 15.2.28.75.1.4. OpenStack;

15.2.28.75.2. Conectores SDN Públicos;

- 15.2.28.75.2.1. Google Cloud Platform (GCP);
- 15.2.28.75.2.2. AWS;
- 15.2.28.75.2.3. Microsoft Azure;
- 15.2.28.75.2.4. Oracle Cloud Infrastructure (OCI);

15.2.28.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).

15.2.28.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;

15.2.28.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).

15.2.28.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.

15.2.28.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

15.2.29. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

15.2.29.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para

as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.

15.2.29.2. Deve permitir modificação de valores DSCP para o DiffServ.

15.2.29.3. Deve permitir priorização de tráfego e suportar ToS.

15.2.29.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.

15.2.29.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.

15.2.29.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.

15.2.29.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.

15.2.29.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.

15.2.29.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.

15.2.29.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

15.2.30. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

15.2.30.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.

15.2.30.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.

15.2.30.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.

15.2.30.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

15.2.30.5. Deve permitir a criação de categorias personalizadas.

15.2.30.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.

15.2.30.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.

15.2.30.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.

15.2.30.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no

Microsoft Active Directory.

- 15.2.30.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 15.2.30.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 15.2.30.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 15.2.30.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 15.2.30.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 15.2.30.15. Permitir a criação de categorias de URLs customizadas;
- 15.2.30.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 15.2.30.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 15.2.30.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 15.2.30.19. Permitir a customização de página de bloqueio;
- 15.2.30.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 15.2.30.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 15.2.30.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 15.2.30.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 15.2.30.24. Permitir e implementar o controle de acesso, habilitando o captive portal,

baseados em políticas definidas pela CONTRATANTE aderente;

- 15.2.30.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 15.2.30.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 15.2.30.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 15.2.30.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 15.2.30.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 15.2.30.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 15.2.30.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 15.2.30.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 15.2.30.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 15.2.30.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 15.2.30.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 15.2.30.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 15.2.30.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 15.2.30.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 15.2.30.39. Deve possuir Proxy Explícito e Transparente.
- 15.2.30.40. Deve implementar roteamento WCCP e ICAP.
- 15.2.31. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)
 - 15.2.31.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.

- 15.2.31.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
- 15.2.31.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 15.2.31.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 15.2.31.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 15.2.31.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 15.2.31.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 15.2.31.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 15.2.31.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 15.2.31.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 15.2.31.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 15.2.31.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 15.2.31.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 15.2.31.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 15.2.31.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 15.2.31.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 15.2.31.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de

anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.

- 15.2.31.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 15.2.31.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 15.2.31.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 15.2.31.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 15.2.31.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 15.2.31.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 15.2.31.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 15.2.31.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 15.2.31.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 15.2.31.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 15.2.31.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 15.2.31.29. Identificar, alertar e bloquear comunicação com botnets;
- 15.2.31.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 15.2.31.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 15.2.31.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de

aplicação ou antimalware;

- 15.2.31.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 15.2.31.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 15.2.31.35. Identificar nos eventos o país de onde partiu a ameaça;
- 15.2.31.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 15.2.31.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 15.2.31.38. Deve possuir alarmes na console de administração.
- 15.2.31.39. Deve possuir alertas via correio eletrônico.
- 15.2.31.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 15.2.31.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 15.2.31.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 15.2.31.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 15.2.31.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;
- 15.2.32. FUNCIONALIDADE DE VPN
 - 15.2.32.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
 - 15.2.32.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
 - 15.2.32.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
 - 15.2.32.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
 - 15.2.32.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
 - 15.2.32.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key

Exchange (IKEv1 e v2);

15.2.32.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;

15.2.32.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);

15.2.32.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;

15.2.32.10. Realizar atribuição de DNS nos clientes remotos de VPN;

15.2.32.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;

15.2.32.12. Suportar leitura e verificação de CRL (Certificate Revocation List);

15.2.32.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;

15.2.32.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;

15.2.32.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;

15.2.32.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.

15.2.32.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSEC estabelecidos.

15.2.33. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

15.2.33.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;

15.2.33.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;

15.2.33.3. Atualizar a base de assinaturas de aplicações automaticamente;

15.2.33.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.

- 15.2.33.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 15.2.33.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 15.2.33.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 15.2.33.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 15.2.33.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 15.2.33.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 15.2.33.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 15.2.33.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensagens instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 15.2.33.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 15.2.33.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 15.2.33.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 15.2.33.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 15.2.33.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.

- 15.2.33.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 15.2.33.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 15.2.33.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 15.2.33.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 15.2.33.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 15.2.33.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 15.2.33.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 15.2.33.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 15.2.33.26. Deve permitir criação de padrões de aplicação manualmente.
- 15.2.33.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 15.2.33.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 15.2.33.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 15.2.33.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;
- 15.2.34. FUNCIONALIDADE DE SD-WAN
 - 15.2.34.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
 - 15.2.34.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.

- 15.2.34.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 15.2.34.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 15.2.34.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 15.2.34.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 15.2.34.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 15.2.34.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 15.2.34.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 15.2.34.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 15.2.34.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 15.2.34.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 15.2.34.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 15.2.34.14. Passivo: uso do tráfego real para as medições;
- 15.2.34.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 15.2.34.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 15.2.34.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo

funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.

- 15.2.34.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 15.2.34.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 15.2.34.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 15.2.34.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 15.2.34.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 15.2.34.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 15.2.34.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 15.2.34.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 15.2.34.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 15.2.34.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da

Interface SD-WAN;

15.2.34.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;

15.2.34.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

15.3. LINK DE CONECTIVIDADE BANDA LARGA EM TRIPLA ABORDAGEM

15.3.1. Deve ser fornecidos três links Banda Larga cada, sendo um com conectividade via satélite e outros dois com conectividade via fibra óptica, para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.

15.3.2. Deve ser utilizados links de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.

15.3.3. Deve ser fornecido 02 (dois) link de internet com conectividade via fibra com velocidade mínima de 500 Mbps de download, e um link com conectividade via satélite com velocidade mínima de 100 Mbps.

15.3.4. Os circuitos de internet terrestre em cada unidade deverão ser entregues cada um por uma operadora ou provedor exclusivo.

15.3.5. Os links devem ser estabelecidos por caminhos completamente distintos, não devendo haver nenhum ponto de falha comum entre os dois links de comunicação.

15.3.6. Deve suportar transporte de pacotes IPv4 e IPv6.

15.3.7. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.

15.3.8. O link deve ser entregue e mantido sem restrições de volume de tráfego.

15.3.9. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.

15.3.10. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.

15.3.11. O link não poderá ter franquia de acesso que limite sua utilização.

15.3.12. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.

15.3.13. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.

- 15.3.14. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 15.3.15. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 15.3.16. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 15.3.17. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 15.3.18. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 15.3.19. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 15.3.20. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 15.3.21. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

15.4. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

- 15.4.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:
 - 15.4.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.
 - 15.4.1.2. Ativação e testes de 02 Links de Internet Banda Larga, assegurando estabilidade e disponibilidade.
 - 15.4.1.3. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.
- 15.4.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:
 - 15.4.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.
 - 15.4.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo

análise de eventos e auditoria.

15.4.2.3. Gerenciamento remoto e centralizado das políticas de segurança de endpoint.

15.4.2.4. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

16.LOTE 01 - ITEM 16 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 16

16.1.A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 16 deve ser implantada em unidades governamentais que necessitam de conectividade segura, proteção de borda, contemplando firewall de próxima geração (NGFW) com tecnologia SD-WAN, três links de internet banda larga, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

16.2. SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW

16.2.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.

16.2.2. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;

16.2.3. Poderá ser feita composição de soluções para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.

16.2.4. Garantir que a solução disponibilize no(s) equipamento(s), acesso a gerência e monitoração, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);

16.2.5. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.

16.2.6. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de

Firewall;

- 16.2.7. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.
- 16.2.8. Deve suportar e estar licenciado para a criação de, ao menos 10(dez) instâncias virtuais de firewall no mesmo hardware.
- 16.2.9. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 16.2.10. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 16.2.11. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 16.2.12. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 16.2.13. Deve possuir firewall com capacidade mínima de processamento de 26 (vinte e seis) Gbps.
- 16.2.14. Deve possuir IPS com capacidade mínima de processamento de 5 (cinco) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 16.2.15. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 2,5 (dois vírgula cinco) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 16.2.16. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 3 (três) Gbps.
- 16.2.17. Deve possuir VPN com capacidade de, pelo menos, 33 (trinta e três) Gbps de tráfego IPSec.

- 16.2.18. Deve suportar 3.000.000 (três milhões) conexões simultâneas.
- 16.2.19. Deve suportar, pelo menos, 135.000 (cento e trinta e cinco mil) novas conexões por segundo.
- 16.2.20. Deve suportar, pelo menos, 1800 (mil e oitocentos) túneis de VPN Site-Site.
- 16.2.21. Deve suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site.
- 16.2.22. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE.
- 16.2.23. Deve possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE.
- 16.2.24. Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.
- 16.2.25. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 16.2.26. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 16.2.27. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.
- 16.2.28. FUNCIONALIDADES DE FIREWALL
 - 16.2.28.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
 - 16.2.28.2. Possuir suporte a sub-interfaces ethernet lógicas;
 - 16.2.28.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
 - 16.2.28.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
 - 16.2.28.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
 - 16.2.28.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
 - 16.2.28.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
 - 16.2.28.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
 - 16.2.28.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
 - 16.2.28.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.

- 16.2.28.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 16.2.28.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 16.2.28.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 16.2.28.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 16.2.28.15. Deve suportar o encaminhamento de tráfego multicast.
- 16.2.28.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 16.2.28.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 16.2.28.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 16.2.28.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 16.2.28.20. Suportar OSPF gracefulrestart;
- 16.2.28.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 16.2.28.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 16.2.28.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 16.2.28.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 16.2.28.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 16.2.28.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 16.2.28.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 16.2.28.28. Drop sem notificação do bloqueio ao usuário;
 - 16.2.28.29. Drop com notificação do bloqueio ao usuário;

- 16.2.28.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
- 16.2.28.31. TCP-Reset para o cliente;
- 16.2.28.32. TCP-Reset para o server ou para os dois lados da conexão.
- 16.2.28.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 16.2.28.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 16.2.28.35. Deve oferecer suporte ao protocolo SIP.
- 16.2.28.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 16.2.28.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 16.2.28.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 16.2.28.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 16.2.28.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 16.2.28.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 16.2.28.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 16.2.28.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 16.2.28.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 16.2.28.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 16.2.28.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de

usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;

- 16.2.28.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 16.2.28.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 16.2.28.49. Realizar Traffic Shaping para a solução de segurança
- 16.2.28.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 16.2.28.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 16.2.28.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 16.2.28.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 16.2.28.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 16.2.28.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 16.2.28.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 16.2.28.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 16.2.28.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 16.2.28.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 16.2.28.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 16.2.28.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 16.2.28.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 16.2.28.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-

spoofing).

- 16.2.28.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 16.2.28.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 16.2.28.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 16.2.28.67. Funcionar com tradução de porta (PAT);
- 16.2.28.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 16.2.28.69. Implementar e suportar NAT64 e NAT46;
- 16.2.28.70. Implementar NAT66
- 16.2.28.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 16.2.28.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 16.2.28.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 16.2.28.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 16.2.28.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:
 - 16.2.28.75.1. Conectores SDN Privados:
 - 16.2.28.75.1.1. Nutanix;
 - 16.2.28.75.1.2. Kubernetes;
 - 16.2.28.75.1.3. VMware ESXi;
 - 16.2.28.75.1.4. OpenStack;
 - 16.2.28.75.2. Conectores SDN Públicos;
 - 16.2.28.75.2.1. Google Cloud Platform (GCP);
 - 16.2.28.75.2.2. AWS;
 - 16.2.28.75.2.3. Microsoft Azure;

16.2.28.75.2.4. Oracle Cloud Infrastructure (OCI);

- 16.2.28.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 16.2.28.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 16.2.28.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).
- 16.2.28.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.
- 16.2.28.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.
- 16.2.29. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO
- 16.2.29.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
- 16.2.29.2. Deve permitir modificação de valores DSCP para o DiffServ.
- 16.2.29.3. Deve permitir priorização de tráfego e suportar ToS.
- 16.2.29.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
- 16.2.29.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 16.2.29.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 16.2.29.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 16.2.29.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 16.2.29.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
- 16.2.29.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

16.2.30. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

- 16.2.30.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
- 16.2.30.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
- 16.2.30.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
- 16.2.30.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 16.2.30.5. Deve permitir a criação de categorias personalizadas.
- 16.2.30.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 16.2.30.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 16.2.30.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 16.2.30.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 16.2.30.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 16.2.30.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 16.2.30.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 16.2.30.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 16.2.30.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 16.2.30.15. Permitir a criação de categorias de URLs customizadas;
- 16.2.30.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 16.2.30.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 16.2.30.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

- 16.2.30.19. Permitir a customização de página de bloqueio;
- 16.2.30.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 16.2.30.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 16.2.30.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 16.2.30.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 16.2.30.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 16.2.30.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 16.2.30.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 16.2.30.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 16.2.30.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 16.2.30.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 16.2.30.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 16.2.30.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 16.2.30.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 16.2.30.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem

interromper a execução dos serviços de filtragem de conteúdo Web.

- 16.2.30.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 16.2.30.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 16.2.30.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 16.2.30.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 16.2.30.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 16.2.30.39. Deve possuir Proxy Explícito e Transparente.
- 16.2.30.40. Deve implementar roteamento WCCP e ICAP.
- 16.2.31. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)
 - 16.2.31.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
 - 16.2.31.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
 - 16.2.31.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
 - 16.2.31.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
 - 16.2.31.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
 - 16.2.31.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
 - 16.2.31.7. Deve permitir funcionar em modo transparente, sniffer e router.
 - 16.2.31.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
 - 16.2.31.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
 - 16.2.31.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
 - 16.2.31.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços

IPs, redes ou zonas de segurança;

- 16.2.31.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 16.2.31.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 16.2.31.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 16.2.31.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 16.2.31.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 16.2.31.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 16.2.31.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 16.2.31.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 16.2.31.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 16.2.31.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 16.2.31.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 16.2.31.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 16.2.31.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 16.2.31.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 16.2.31.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;

- 16.2.31.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 16.2.31.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 16.2.31.29. Identificar, alertar e bloquear comunicação com botnets;
- 16.2.31.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 16.2.31.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 16.2.31.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 16.2.31.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 16.2.31.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 16.2.31.35. Identificar nos eventos o país de onde partiu a ameaça;
- 16.2.31.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 16.2.31.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 16.2.31.38. Deve possuir alarmes na console de administração.
- 16.2.31.39. Deve possuir alertas via correio eletrônico.
- 16.2.31.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 16.2.31.41. Deve ter a capacidade de resposta/logs ativa a ataques.

- 16.2.31.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 16.2.31.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 16.2.31.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

16.2.32. FUNCIONALIDADE DE VPN

- 16.2.32.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
- 16.2.32.2. Suportar nativamente a criação de VPN IPsec utilizando 3DES;
- 16.2.32.3. Suportar nativamente a criação de VPN IPsec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
- 16.2.32.4. Suportar nativamente a autenticação de VPN IPsec utilizando MD5 e SHA-1;
- 16.2.32.5. Suportar nativamente a criação de VPN IPsec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
- 16.2.32.6. Suportar nativamente a criação de VPN IPsec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
- 16.2.32.7. Suportar nativamente, para VPN IPsec, autenticação via certificado IKE PKI;
- 16.2.32.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPsec a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 16.2.32.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 16.2.32.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 16.2.32.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 16.2.32.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 16.2.32.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 16.2.32.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 16.2.32.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 16.2.32.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos:

Windows, Linux e Mac OS.

- 16.2.32.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSec estabelecidos.

16.2.33. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

- 16.2.33.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
- 16.2.33.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
- 16.2.33.3. Atualizar a base de assinaturas de aplicações automaticamente;
- 16.2.33.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
- 16.2.33.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 16.2.33.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 16.2.33.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 16.2.33.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 16.2.33.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 16.2.33.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 16.2.33.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 16.2.33.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 16.2.33.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria,

uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.

- 16.2.33.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 16.2.33.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 16.2.33.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 16.2.33.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 16.2.33.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 16.2.33.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 16.2.33.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 16.2.33.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 16.2.33.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 16.2.33.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 16.2.33.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 16.2.33.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 16.2.33.26. Deve permitir criação de padrões de aplicação manualmente.
- 16.2.33.27. Deve permitir criar assinaturas personalizadas com o uso de expressões

regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;

- 16.2.33.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 16.2.33.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 16.2.33.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;

16.2.34. FUNCIONALIDADE DE SD-WAN

- 16.2.34.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
- 16.2.34.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.
- 16.2.34.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 16.2.34.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 16.2.34.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 16.2.34.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 16.2.34.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 16.2.34.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 16.2.34.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 16.2.34.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de

pacote de dados;

- 16.2.34.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 16.2.34.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 16.2.34.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 16.2.34.14. Passivo: uso do tráfego real para as medições;
- 16.2.34.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 16.2.34.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 16.2.34.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 16.2.34.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 16.2.34.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 16.2.34.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 16.2.34.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 16.2.34.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).

- 16.2.34.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 16.2.34.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 16.2.34.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 16.2.34.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 16.2.34.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 16.2.34.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 16.2.34.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

16.3. LINK DE CONECTIVIDADE BANDA LARGA EM TRIPLA ABORDAGEM

- 16.3.1. Deve ser fornecidos três links Banda Larga cada, sendo um com conectividade via satélite e outros dois com conectividade via fibra óptica, para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.
- 16.3.2. Deve ser utilizados links de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances SD-WAN.
- 16.3.3. Deve ser fornecido 02 (dois) link de internet com conectividade via fibra com velocidade mínima de 1 Gbps de download, e um link com conectividade via satélite com velocidade mínima de 100 Mbps.

- 16.3.4. Os circuitos de internet terrestre em cada unidade deverão ser entregues cada um por uma operadora ou provedor exclusivo.
- 16.3.5. Os links devem ser estabelecidos por caminhos completamente distintos, não devendo haver nenhum ponto de falha comum entre os dois links de comunicação.
- 16.3.6. Deve suportar transporte de pacotes IPv4 e IPv6.
- 16.3.7. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 16.3.8. O link deve ser entregue e mantido sem restrições de volume de tráfego.
- 16.3.9. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 16.3.10. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 16.3.11. O link não poderá ter franquia de acesso que limite sua utilização.
- 16.3.12. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 16.3.13. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.
- 16.3.14. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 16.3.15. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 16.3.16. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 16.3.17. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 16.3.18. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.
- 16.3.19. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 16.3.20. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 16.3.21. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para

esse fim.

16.4. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

16.4.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:

16.4.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.

16.4.1.2. Ativação e testes de 02 Links de Internet Banda Larga, assegurando estabilidade e disponibilidade.

16.4.1.3. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

16.4.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:

16.4.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.

16.4.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.

16.4.2.3. Gerenciamento remoto e centralizado das políticas de segurança de endpoint.

16.4.2.4. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

17. LOTE 01 - ITEM 17 - SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 17

17.1.A SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 17 deve ser implantada em unidades governamentais que necessitam de conectividade segura que possuam até 05 devices, com link de internet banda larga, com integração total ao ambiente de gerenciamento centralizado. Conforme requisitos abaixo:

17.2. LINK DE CONECTIVIDADE BANDA LARGA

17.2.1. O link de 200 Mbps Banda Larga serão fornecidos para garantir conectividade confiável e contínua para as unidades contempladas no escopo do projeto.

17.2.2. Deve ser utilizado link de comunicação terrestre confeccionados com fibra óptica para acesso de última milha. Apenas será permitida a conversão do meio óptico para par metálico (UTP) para compatibilização com as interfaces dos CPEs, ou seja, roteadores ou appliances

SD-WAN.

- 17.2.3. Deve ser fornecido 01 (um) link de internet com velocidade mínima de 200 Mbps de download.
- 17.2.4. Para os locais em que não houver viabilidade técnica disponibilizar link de conectividade fibra óptica, será aceito a entrega de link via conectividade via rádio e ou satélite, desde que comprovado o não atendimento e mediante a aprovação da CONTRANTE para substituição do meio.
- 17.2.5. O link de internet Banda Larga fornecido deverá disponibilizar um CPE que permita o monitoramento através de SNMP V3 além endereçamento IP fixo em IPv6, válido e roteável na Internet, atribuído exclusivamente ao CONTRATANTE, não sendo permitido o uso de endereçamento dinâmico, NAT ou CGNAT para o tráfego IPv6.
- 17.2.6. Deve suportar transporte de pacotes IPv4 e IPv6.
- 17.2.7. Deve atender às Taxas de Transmissão Média e Instantânea (download e upload) iguais ou superiores aos limites estabelecidos pela ANATEL.
- 17.2.8. O link deve ser entregue e mantido sem restrições de volume de tráfego.
- 17.2.9. Deve disponibilizar serviço de DNS da Contratada, com suporte para resolução direta e reversa de endereços IPv4 e IPv6.
- 17.2.10. Não será permitida a utilização de tecnologias 3G e 4G para a conectividade do link.
- 17.2.11. O link não poderá ter franquia de acesso que limite sua utilização.
- 17.2.12. Não será aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 17.2.13. A Contratante poderá auditar a capacidade efetiva de navegação através de ferramentas próprias ou fornecidas pela Contratada.
- 17.2.14. A Contratada não poderá executar qualquer tipo de filtro ou proxy sobre o tráfego originado ou destinado à rede da Contratante.
- 17.2.15. O serviço deve permitir a criação de VPNs (Virtual Private Network) sem necessidade de liberação ou intervenção da Contratada.
- 17.2.16. Os equipamentos e links fornecidos deverão obedecer às normas e recomendações vigentes de órgãos oficiais competentes.
- 17.2.17. O acesso de última milha deve ser realizado por links de comunicação terrestre em fibra óptica, permitindo conversão para par metálico (UTP) apenas para compatibilidade com os equipamentos.
- 17.2.18. A Contratada será responsável pela instalação e ativação da infraestrutura necessária nos locais indicados pela Contratante.

- 17.2.19. A passagem de cabos e fibras pela fachada dos prédios sem tubulação própria será expressamente vedada.
- 17.2.20. O link deve ser capaz de suportar tráfego com banda completamente ocupada sem degradação de desempenho.
- 17.2.21. Expressamente vedada a passagem de cabos e fibras pela fachada dos prédios, sem tubulação própria e com adaptações precárias/provisórias para instalação dos circuitos de internet. Devem ser utilizadas as infraestruturas e tubulações de entradas específicas para esse fim.

17.3. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

- 17.3.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:
 - 17.3.1.1. Ativação e testes de 01 Link de Internet Banda Larga, assegurando estabilidade e disponibilidade.
 - 17.3.1.2. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

18. LOTE 01 - ITEM 18 – SERVIÇO DE MUDANÇA DE ENDEREÇO – ATÉ 300 KM DE SALVADOR/BA

- 18.1. Desinstalação lógica e física, transporte seguro e reinstalação da Solução de Conectividade (Firewall, SD-WAN, Roteadores) no novo endereço. Inclui configuração lógica para restabelecimento do serviço e testes de conectividade para Capital e localidades até 300 km de Salvador Bahia:
 - 18.1.1. Os serviços de mudanças de endereço estarão sujeitos a viabilidade técnica para atendimento no novo local, devendo ser realizada Vistoria Técnica para verificação de viabilidade técnica de mudança de Endereço da Solução de Conectividade (Firewall e Links de Conectividade) para Capital e localidades até 300 km de Salvador Bahia.
 - 18.1.1.1. Nos casos em que for constatada inviabilidade técnica, devidamente comprovada, para atendimento por meio de conectividade em fibra óptica no endereço solicitado, a CONTRATADA deverá encaminhar à CONTRATANTE justificativa técnica formal para análise e validação. A avaliação da impossibilidade de atendimento caberá à CONTRATANTE, que poderá, a seu critério, deliberar pela adoção de solução alternativa, incluindo a substituição por conectividade via rádio e/ou satélite, com o objetivo de

assegurar a continuidade da prestação do serviço. A utilização de soluções alternativas somente será permitida mediante aprovação prévia da CONTRATANTE, condicionada à devida comprovação técnica da inviabilidade. Fica estabelecido que o quantitativo de acessos classificados como tecnicamente inviáveis e atendidos por meio alternativo (rádio e/ou satélite) estará limitado a até 5% (cinco por cento) do total de acessos previstos em cada contrato. Nos casos em que a aplicação desse percentual resultar em número fracionado, o valor deverá ser arredondado para o número inteiro imediatamente superior.

18.1.1.2.

18.2. DINÂMICA DE CONTRATAÇÃO:

- 18.2.1. O prazo máximo para início das atividades pela empresa contratada será de 10 (vinte) dias uteis;
- 18.2.2. A empresa CONTRATADA deve nomear funcionário capacitado que será responsável por fornecer aconselhamento técnico e operacional sobre os serviços; assistência sobre as condições do contrato; gerenciamento de escalação junto ao Fabricante; Gerenciamento de recursos e cronograma de entrega dos serviços;
- 18.2.3. Neste modelo de execução dos serviços não se caracteriza a subordinação direta e nem a pessoalidade, visto que não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da empresa contratada e este Órgão. As empresas proponentes deverão considerar em seus custos todos os recursos necessários ao completo atendimento aos objetos, tais como despesas com pessoal (salários, férias, encargos, benefícios, seleção, outras) de modo a garantir os serviços definidos;

18.3. ETAPAS:

18.3.1. Iniciação:

- 18.3.1.1. Avaliação do cenário da CONTRATANTE: Realização de uma análise completa do ambiente do cliente para entender suas necessidades específicas.
- 18.3.1.2. Desenvolvimento de plano de implementação: Criação de um plano detalhado que delinea as etapas e os recursos necessários para a implementação bem-sucedida do projeto.

18.3.2. Planejamento:

- 18.3.2.1. Elaboração de uma estratégia abrangente que inclui o cronograma de implementação, controle de prazos, esforço, vistoria, atribuição de responsabilidades, alocação de recursos, indicadores do projeto e qualquer outra métrica prevista no PMBOK. O objetivo

de todas estas atividades é a garantia de qualidade do projeto no que tange prazos e esforço.

18.3.3. Execução:

18.3.3.1. Análise: Realização de uma análise minuciosa dos requisitos e processos da CONTRATANTE para garantir que a solução proposta seja adequada.

18.3.3.2. Configuração: Personalização da solução de acordo com as necessidades específicas da CONTRATANTE ajustando as configurações e os parâmetros de rede.

18.3.3.3. Integração: Integração da solução com os sistemas existentes, garantindo a interoperabilidade e o fluxo de dados adequado.

18.3.3.4. Testes, otimização e ajustes: Realização de testes para verificar a funcionalidade e estabilidade da solução implantada. A partir dos resultados, implementamos melhorias e ajustes para otimizar o desempenho e garantir o resultado esperado.

18.3.4. Encerramento:

18.3.4.1. Documentação: Elaboração de documentação que descreve a solução implantada conforme construída.

19.LOTE 01 - ITEM 19 – SERVIÇO DE MUDANÇA DE ENDEREÇO – ACIMA DE 300 KM ATÉ 600 KM DE SALVADOR/BA

19.1.Desinstalação lógica e física, transporte seguro e reinstalação da Solução de Conectividade (Firewall, SD-WAN, Roteadores) no novo endereço. Inclui configuração lógica para restabelecimento do serviço e testes de conectividade para localidades acima de 300KM e até 600 km de Salvador Bahia;

19.1.1. Os serviços de mudanças de endereço estarão sujeitos a viabilidade técnica para atendimento no novo local, devendo ser realizada Vistoria Técnica para verificação de viabilidade técnica de mudança de Endereço da Solução de Conectividade (Firewall e Links de Conectividade) para Capital e localidades até 300 km de Salvador Bahia.

19.1.1.1. Nos casos em que for constatada inviabilidade técnica, devidamente comprovada, para atendimento por meio de conectividade em fibra óptica no endereço solicitado, a CONTRATADA deverá encaminhar à CONTRATANTE justificativa técnica formal para análise e validação. A avaliação da impossibilidade de atendimento caberá à CONTRATANTE, que poderá, a seu critério, deliberar pela adoção de solução alternativa, incluindo a substituição por conectividade via rádio e/ou satélite, com o objetivo de assegurar a continuidade da prestação do serviço. A utilização de soluções alternativas

somente será permitida mediante aprovação prévia da CONTRATANTE, condicionada à devida comprovação técnica da inviabilidade. Fica estabelecido que o quantitativo de acessos classificados como tecnicamente inviáveis e atendidos por meio alternativo (rádio e/ou satélite) estará limitado a até 5% (cinco por cento) do total de acessos previstos em cada contrato. Nos casos em que a aplicação desse percentual resultar em número fracionado, o valor deverá ser arredondado para o número inteiro imediatamente superior.

19.2. DINÂMICA DE CONTRATAÇÃO:

- 19.2.1. O prazo máximo para início das atividades pela empresa contratada será de 10 (vinte) dias úteis;
- 19.2.2. A empresa CONTRATADA deve nomear funcionário capacitado que será responsável por fornecer aconselhamento técnico e operacional sobre os serviços; assistência sobre as condições do contrato; gerenciamento de escalação junto ao Fabricante; Gerenciamento de recursos e cronograma de entrega dos serviços;
- 19.2.3. Neste modelo de execução dos serviços não se caracteriza a subordinação direta e nem a pessoalidade, visto que não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da empresa contratada e este Órgão. As empresas proponentes deverão considerar em seus custos todos os recursos necessários ao completo atendimento aos objetos, tais como despesas com pessoal (salários, férias, encargos, benefícios, seleção, outras) de modo a garantir os serviços definidos;

19.3. ETAPAS:

- 19.3.1. Iniciação:
 - 19.3.1.1. Avaliação do cenário da CONTRATANTE: Realização de uma análise completa do ambiente do cliente para entender suas necessidades específicas.
 - 19.3.1.2. Desenvolvimento de plano de implementação: Criação de um plano detalhado que delinea as etapas e os recursos necessários para a implementação bem-sucedida do projeto.
- 19.3.2. Planejamento:
 - 19.3.2.1. Elaboração de uma estratégia abrangente que inclui o cronograma de implementação, controle de prazos, esforço, vistoria, atribuição de responsabilidades, alocação de recursos, indicadores do projeto e qualquer outra métrica prevista no PMBOK. O objetivo de todas estas atividades é a garantia de qualidade do projeto no que tange prazos e

esforço.

19.3.3. Execução:

19.3.3.1. Análise: Realização de uma análise minuciosa dos requisitos e processos da CONTRATANTE para garantir que a solução proposta seja adequada.

19.3.3.2. Configuração: Personalização da solução de acordo com as necessidades específicas da CONTRATANTE ajustando as configurações e os parâmetros de rede.

19.3.3.3. Integração: Integração da solução com os sistemas existentes, garantindo a interoperabilidade e o fluxo de dados adequado.

19.3.3.4. Testes, otimização e ajustes: Realização de testes para verificar a funcionalidade e estabilidade da solução implantada. A partir dos resultados, implementamos melhorias e ajustes para otimizar o desempenho e garantir o resultado esperado.

19.3.4. Encerramento:

19.3.4.1. Documentação: Elaboração de documentação que descreve a solução implantada conforme construída.

20.LOTE 01– ITEM 20 – SERVIÇO DE MUDANÇA DE ENDEREÇO – ACIMA DE 600 KM DE SALVADOR/BA

20.1.Desinstalação lógica e física, transporte seguro e reinstalação da Solução de Conectividade (Firewall, SD-WAN, Roteadores) no novo endereço. Inclui configuração lógica para restabelecimento do serviço e testes de conectividade para localidades acima de 300 km de Salvador Bahia:

20.1.1. Os serviços de mudanças de endereço estarão sujeitos a viabilidade técnica para atendimento no novo local, devendo ser realizada Vistoria Tecnica para verificação de viabilidade técnica de mudança de Endereço da Solução de Conectividade (Firewall e Links de Conectividade) para Capital e localidades até 300 km de Salvador Bahia.

20.1.1.1. Nos casos em que for constatada inviabilidade técnica, devidamente comprovada, para atendimento por meio de conectividade em fibra óptica no endereço solicitado, a CONTRATADA deverá encaminhar à CONTRATANTE justificativa técnica formal para análise e validação. A avaliação da impossibilidade de atendimento caberá à CONTRATANTE, que poderá, a seu critério, deliberar pela adoção de solução alternativa, incluindo a substituição por conectividade via rádio e/ou satélite, com o objetivo de assegurar a continuidade da prestação do serviço. A utilização de soluções alternativas somente será permitida mediante aprovação prévia da CONTRATANTE, condicionada à

devida comprovação técnica da inviabilidade. Fica estabelecido que o quantitativo de acessos classificados como tecnicamente inviáveis e atendidos por meio alternativo (rádio e/ou satélite) estará limitado a até 5% (cinco por cento) do total de acessos previstos em cada contrato. Nos casos em que a aplicação desse percentual resultar em número fracionado, o valor deverá ser arredondado para o número inteiro imediatamente superior.

20.2. DINÂMICA DE CONTRATAÇÃO:

- 20.2.1. O prazo máximo para início das atividades pela empresa contratada será de 10 (vinte) dias úteis;
- 20.2.2. A empresa CONTRATADA deve nomear funcionário capacitado que será responsável por fornecer aconselhamento técnico e operacional sobre os serviços; assistência sobre as condições do contrato; gerenciamento de escalação junto ao Fabricante; Gerenciamento de recursos e cronograma de entrega dos serviços;
- 20.2.3. Neste modelo de execução dos serviços não se caracteriza a subordinação direta e nem a personalidade, visto que não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da empresa contratada e este Órgão. As empresas proponentes deverão considerar em seus custos todos os recursos necessários ao completo atendimento aos objetos, tais como despesas com pessoal (salários, férias, encargos, benefícios, seleção, outras) de modo a garantir os serviços definidos;

20.3. ETAPAS:

- 20.3.1. Iniciação:
 - 20.3.1.1. Avaliação do cenário da CONTRATANTE: Realização de uma análise completa do ambiente do cliente para entender suas necessidades específicas.
 - 20.3.1.2. Desenvolvimento de plano de implementação: Criação de um plano detalhado que delinea as etapas e os recursos necessários para a implementação bem-sucedida do projeto.
- 20.3.2. Planejamento:
 - 20.3.2.1. Elaboração de uma estratégia abrangente que inclui o cronograma de implementação, controle de prazos, esforço, vistoria, atribuição de responsabilidades, alocação de recursos, indicadores do projeto e qualquer outra métrica prevista no PMBOK. O objetivo de todas estas atividades é a garantia de qualidade do projeto no que tange prazos e esforço.

20.3.3. Execução:

20.3.3.1. Análise: Realização de uma análise minuciosa dos requisitos e processos da CONTRATANTE para garantir que a solução proposta seja adequada.

20.3.3.2. Configuração: Personalização da solução de acordo com as necessidades específicas da CONTRATANTE ajustando as configurações e os parâmetros de rede.

20.3.3.3. Integração: Integração da solução com os sistemas existentes, garantindo a interoperabilidade e o fluxo de dados adequado.

20.3.3.4. Testes, otimização e ajustes: Realização de testes para verificar a funcionalidade e estabilidade da solução implantada. A partir dos resultados, implementamos melhorias e ajustes para otimizar o desempenho e garantir o resultado esperado.

20.3.4. Encerramento:

20.3.4.1. Documentação: Elaboração de documentação que descreve a solução implantada conforme construída.

21.LOTE 01 - ITEM 21 - SOLUÇÃO DE OPERAÇÃO, GERENCIAMENTO E MONITORAMENTO CENTRAL

21.1.ESCOPO DOS SERVIÇOS DE OPERAÇÃO, GERENCIAMENTO E MONITORAMENTO

21.1.1. Os serviços a serem contratados referem-se ao modelo de Infraestrutura como Serviço (IaaS), contemplando o fornecimento, implantação, operação e sustentação de uma solução integrada de conectividade segura para unidades governamentais do Estado da Bahia, com vigência contratual de 60 (sessenta) meses. A infraestrutura abrangerá proteção avançada de rede e dispositivos, além de um centro unificado de monitoramento da solução;

21.1.2. Os serviços descritos corresponderão a operação, monitoramento e sustentação para contratações de até 500 (quinhentas) soluções de conectividade segura. Para quantitativos superiores, a CONTRATANTE deverá contratar unidade adicional deste item, de forma a suportar o novo volume de SOLUÇÕES DE CONECTIVIDADE SEGURA;

21.1.2.1. Para início das atividades de SOLUÇÃO DE OPERAÇÃO, GERENCIAMENTO E MONITORAMENTO CENTRAL a PRODEB deverá contratar 03(três) unidades deste item, permitindo assim a operação e o monitoramento inicial, operação e monitoramento de 1500 (mil e quinhentos) devices.

21.1.3. Este centro será responsável pela coleta de eventos, aplicação de políticas, supervisão contínua da segurança e tráfego, bem como pela interface com a equipe técnica da PRODEB;

21.1.4. Os subitens "18.7.SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO" e "NGFW

18.9.PLATAFORMA CENTRALIZADA DE GERENCIAMENTO DE DISPOSITIVOS”, devem ser fornecidos de maneira total e única na primeira contratação da “SOLUÇÃO DE OPERAÇÃO , GERENCIAMENTO E MONITORAMENTO CENTRAL”, não sendo necessários novos fornecimentos em futuras contratações deste item.

21.2.FORNECIMENTO DE SOLUÇÕES DE CONECTIVIDADE SEGURA PARA UNIDADES GOVERNAMENTAIS:

- 21.2.1. As unidades governamentais serão atendidas com soluções, de acordo com seu porte, infraestrutura existente e necessidades operacionais. As soluções contemplam diferentes combinações dos seguintes componentes:
- 21.2.2. Link de internet de alta velocidade, com largura de banda proporcional ao perfil da unidade;
- 21.2.3. Firewall de próxima geração (NGFW) para inspeção de tráfego e políticas de controle;
- 21.2.4. Solução de acesso seguro baseada em confiança zero (ZTA);
- 21.2.5. Monitoramento remoto e suporte especializado durante toda a vigência contratual.

21.3.GERENCIAMENTO, MONITORAMENTO E SUPORTE TÉCNICO ESPECIALIZADO

- 21.3.1. Prestação de serviços contínuos de operação, gerenciamento e monitoramento da infraestrutura, abrangendo:
 - 21.3.1.1. Provisionamento inicial e configuração;
 - 21.3.1.2. Monitoramento proativo 24x7;
 - 21.3.1.3. Manutenção preventiva e corretiva.
 - 21.3.1.4. Atendimento técnico especializado com níveis de serviço (SLA) definidos para incidentes críticos e não críticos, com abertura automática de chamados e suporte remoto/especializado conforme item 6, Acordo de Nível de Serviço deste termo de referência.
 - 21.3.1.5. Geração de relatórios periódicos com indicadores de disponibilidade, desempenho, segurança e uso dos recursos, acompanhados de recomendações de melhoria contínua.

21.4.LOGÍSTICA E EXECUÇÃO DOS SERVIÇOS

- 21.4.1. A CONTRATADA será responsável por todo o deslocamento e atividades logísticas necessárias à instalação, manutenção preventiva e corretiva dos equipamentos, incluindo transporte, seguro, embalagem e quaisquer custos associados;
- 21.4.2. Todos os serviços deverão assegurar plena conectividade, interoperabilidade e segurança da rede implantada, atendendo aos objetivos estratégicos das unidades governamentais do Estado da Bahia.

21.5.EXIGÊNCIAS TÉCNICAS E OPERACIONAIS

- 21.5.1. A CONTRATADA deverá designar um Preposto do Contrato, responsável por atuar como ponto focal entre a equipe técnica da CONTRATADA e a PRODEB BA, especialmente em casos de escalonamento, falhas de atendimento ou incidentes críticos.
- 21.5.2. A LICITANTE não poderá ceder ou transferir, no todo ou em parte, os compromissos assumidos no âmbito deste contrato.
- 21.5.3. A LICITANTE deverá apresentar documentação pública ou técnica que comprove as funcionalidades mínimas exigidas para os equipamentos ofertados, conforme as especificações detalhadas.
- 21.5.4. Todos os componentes e acessórios fornecidos deverão ser entregues instalados, configurados e em pleno funcionamento, conforme projeto executivo aprovado.
- 21.5.5. Antes de qualquer serviço de instalação, a CONTRATADA deverá realizar uma vistoria técnica prévia na unidade para verificação de viabilidade, infraestrutura física e análise de risco técnico.
- 21.5.6. Essa vistoria deverá ser agendada previamente com no mínimo 24 (vinte e quatro) horas de antecedência, em conjunto com o responsável designado pela PRODEB-BA.
- 21.5.7. Após cada intervenção, a CONTRATADA deverá entrar em contato com o responsável técnico da PRODEB -BA para que este homologue os serviços executados.
- 21.5.8. Os serviços de instalação e manutenção não devem comprometer o funcionamento das atividades. É responsabilidade da CONTRATADA realizar a recomposição completa dos ambientes ao término das atividades, inclusive em casos de danos físicos causados durante a execução dos serviços.
- 21.5.9. Durante os serviços, os locais de trabalho devem ser mantidos organizados, desobstruídos e sinalizados, garantindo a segurança da comunidade.
- 21.5.10. Após os serviços, a área de intervenção deve ser limpa e livre de resíduos, sobras de material ou impurezas.
- 21.5.11. A CONTRATADA deverá apresentar planilhas de execução individualizadas por unidade, contendo:
 - 21.5.11.1. Relação detalhada dos equipamentos e componentes instalados;
 - 21.5.11.2. Desempenho previsto;
 - 21.5.11.3. Procedimentos técnicos realizados;
 - 21.5.11.4. Instrumentos e parâmetros utilizados nos testes de validação.
- 21.5.12. A eventual recusa na aceitação dos serviços deverá ser formalizada por escrito pela

PRODEB -BA, detalhando os motivos da não conformidade e os itens rejeitados. A CONTRATADA deverá proceder com os ajustes, substituições ou correções necessárias e reapresentar os serviços para nova homologação.

21.5.13. Caso não haja manifestação da PRODEB -BA no prazo estabelecido, os serviços serão considerados automaticamente aceitos. No entanto, a PRODEB -BA reserva-se o direito de exigir, durante a vigência contratual, a substituição de qualquer componente que apresente falhas recorrentes ou não atenda ao desempenho exigido.

21.5.14. A CONTRATADA deverá disponibilizar equipe técnica qualificada para instalação, configuração e suporte da solução, composta por profissionais com certificação e capacitação comprovada pelo fabricante para operar os equipamentos e soluções ofertadas.

21.5.15. Todos os itens e serviços contratados deverão ter garantia mínima de 60 (sessenta) meses.

21.5.16. Os chamados de suporte deverão ser abertos diretamente com a CONTRATADA, por meio de:

21.5.16.1. Canal telefônico gratuito (0800 ou equivalente);

21.5.16.2. Portal WEB de atendimento;

21.5.16.3. O número do chamado, data e hora de abertura devem ser registrados e considerados como ponto de partida para contagem dos prazos conforme item 6, Acordo de Nível de Serviço deste termo de referência.

21.5.16.4. Durante todo o período de garantia, o serviço de suporte técnico deve operar em regime 24 x 7.

21.5.17. A CONTRATADA deverá fornecer acesso à plataforma do fabricante para download de drivers, atualizações e documentação técnica.

21.5.18. Todo serviço de suporte deve ser realizado por profissional certificado pelo fabricante.

21.5.19. O serviço de suporte deverá proporcionar interação direta com a equipe técnica da PRODEB-BA, garantindo apoio na resolução de incidentes e pronto restabelecimento da operação das unidades.

21.5.20. Ao final da implantação ou manutenção, deverão ser realizados testes funcionais completos, com validação do correto funcionamento da solução em conformidade com as especificações e boas práticas do setor.

21.6. CENTRO DE MONITORAMENTO INTEGRADO

21.6.1. Deve ser realizado o fornecimento e a implantação de Centro de Monitoramento Integrado em local adequado indicado pela PRODEB. O centro de controle será responsável

pela segurança de rede e monitoramento centralizado de todos os equipamentos, serviços e conexões relacionados à infraestrutura de conectividade segura das unidades contempladas neste projeto. Devendo ser implementado no Centro de Monitoramento Integrado os seguintes componentes e serviços:

21.6.1.1. SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW

- 21.6.1.1.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux;
- 21.6.1.1.2. Poderá ser feita composição de soluções para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração;
- 21.6.1.1.3. A solução - a serem configurados em cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados para funcionar dessa forma;
- 21.6.1.1.4. Deve possuir e estar licenciado durante a vigência contratual de 60 (sessenta) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e contextos virtuais;
- 21.6.1.1.5. Deve possuir fonte de alimentação redundante hot swappable com chaveamento automático 110/220V. A fonte fornecida deve suportar sozinha a operação da unidade com todos os módulos de interface ativos;
- 21.6.1.1.6. Deve possuir firewall com capacidade mínima de processamento de 130 (cento e trinta) Gbps;
- 21.6.1.1.7. Deve possuir IPS com capacidade mínima de processamento de 20 (vinte) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 21.6.1.1.8. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 14 (quatorze) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas;

- 21.6.1.1.9. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 11 (onze) Gbps;
- 21.6.1.1.10. Deve possuir VPN com capacidade de, pelo menos, 50 (cinquenta) Gbps de tráfego IPSec;
- 21.6.1.1.11. Deve suportar 10.000.000 (dez milhões) conexões simultâneas;
- 21.6.1.1.12. Deve suportar, pelo menos, 600.000 (seiscentos mil) novas conexões por segundo;
- 21.6.1.1.13. Deve suportar, pelo menos, 18.000 (dezoito mil) túneis de VPN Site-Site;
- 21.6.1.1.14. Deve suportar, pelo menos, 80.000 (oitenta mil) túneis de VPN Client-Site;
- 21.6.1.1.15. Deve possuir, pelo menos, 02 (duas) interfaces QSFP28 100GE;
- 21.6.1.1.16. Deve possuir, pelo menos, 5 (cinco) interfaces SFP28 25GE;
- 21.6.1.1.17. Deve possuir, pelo menos, 5 (cinco) interfaces SFP+ 10GE;
- 21.6.1.1.18. Deve possuir, pelo menos, 08 (oito) interfaces SFP 1GE;
- 21.6.1.1.19. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE;
- 21.6.1.1.20. Deve suportar no mínimo 20 (vinte) instâncias virtuais de firewall e estar licenciado para no mínimo 10 (dez) instâncias virtuais de firewall;
- 21.6.1.1.21. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 21.6.1.1.22. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual;
- 21.6.1.1.23. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês;
- 21.6.1.1.24. FUNCIONALIDADE DE FIREWALL
 - 21.6.1.1.24.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.
 - 21.6.1.1.24.2. Possuir suporte a sub-interfaces ethernet lógicas;
 - 21.6.1.1.24.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
 - 21.6.1.1.24.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.

- 21.6.1.1.24.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 21.6.1.1.24.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 21.6.1.1.24.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 21.6.1.1.24.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 21.6.1.1.24.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 21.6.1.1.24.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 21.6.1.1.24.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 21.6.1.1.24.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 21.6.1.1.24.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 21.6.1.1.24.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 21.6.1.1.24.15. Deve suportar o encaminhamento de tráfego multicast.
- 21.6.1.1.24.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 21.6.1.1.24.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 21.6.1.1.24.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 21.6.1.1.24.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 21.6.1.1.24.20. Suportar OSPF gracefulrestart;
- 21.6.1.1.24.21. Suportar Modo Sniffer, para inspeção via porta espelhada do

tráfego de dados da rede;

- 21.6.1.1.24.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 21.6.1.1.24.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 21.6.1.1.24.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 21.6.1.1.24.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 21.6.1.1.24.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 21.6.1.1.24.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 21.6.1.1.24.28. Drop sem notificação do bloqueio ao usuário;
 - 21.6.1.1.24.29. Drop com notificação do bloqueio ao usuário;
 - 21.6.1.1.24.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 21.6.1.1.24.31. TCP-Reset para o cliente;
 - 21.6.1.1.24.32. TCP-Reset para o server ou para os dois lados da conexão.
- 21.6.1.1.24.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 21.6.1.1.24.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 21.6.1.1.24.35. Deve oferecer suporte ao protocolo SIP.
- 21.6.1.1.24.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 21.6.1.1.24.37. Deve permitir a definição de serviços com base em portas ou

conjunto de portas dos protocolos TCP, UDP, ICMP e IP.

- 21.6.1.1.24.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 21.6.1.1.24.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 21.6.1.1.24.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 21.6.1.1.24.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 21.6.1.1.24.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 21.6.1.1.24.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 21.6.1.1.24.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 21.6.1.1.24.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 21.6.1.1.24.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 21.6.1.1.24.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 21.6.1.1.24.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 21.6.1.1.24.49. Realizar Traffic Shaping para a solução de segurança
- 21.6.1.1.24.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;

- 21.6.1.1.24.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 21.6.1.1.24.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 21.6.1.1.24.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 21.6.1.1.24.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 21.6.1.1.24.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 21.6.1.1.24.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 21.6.1.1.24.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 21.6.1.1.24.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 21.6.1.1.24.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 21.6.1.1.24.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 21.6.1.1.24.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 21.6.1.1.24.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 21.6.1.1.24.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 21.6.1.1.24.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 21.6.1.1.24.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 21.6.1.1.24.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional

1-to-1);

- 21.6.1.1.24.67. Funcionar com tradução de porta (PAT);
- 21.6.1.1.24.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 21.6.1.1.24.69. Implementar e suportar NAT64 e NAT46;
- 21.6.1.1.24.70. Implementar NAT66
- 21.6.1.1.24.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 21.6.1.1.24.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 21.6.1.1.24.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 21.6.1.1.24.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 21.6.1.1.24.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:
 - 21.6.1.1.24.76. Conectores SDN Privados:
 - 21.6.1.1.24.77. Nutanix;
 - 21.6.1.1.24.78. Kubernetes;
 - 21.6.1.1.24.79. VMware ESXi;
 - 21.6.1.1.24.80. OpenStack;
 - 21.6.1.1.24.81. Conectores SDN Públicos;
 - 21.6.1.1.24.82. Google Cloud Platform (GCP);
 - 21.6.1.1.24.83. AWS;
 - 21.6.1.1.24.84. Microsoft Azure;
 - 21.6.1.1.24.85. Oracle Cloud Infrastructure (OCI);

- 21.6.1.1.24.86. Deve permitir a comunicação de acesso administrativo ao equipamento seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 21.6.1.1.24.87. Garantir que o acesso administrativo e monitoramento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 21.6.1.1.24.88. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).
- 21.6.1.1.24.89. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.
- 21.6.1.1.24.90. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.
- 21.6.1.1.25. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO
 - 21.6.1.1.25.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
 - 21.6.1.1.25.2. Deve permitir modificação de valores DSCP para o DiffServ.
 - 21.6.1.1.25.3. Deve permitir priorização de tráfego e suportar ToS.
 - 21.6.1.1.25.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
 - 21.6.1.1.25.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
 - 21.6.1.1.25.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
 - 21.6.1.1.25.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
 - 21.6.1.1.25.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
 - 21.6.1.1.25.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.

21.6.1.1.25.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

21.6.1.1.26. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

21.6.1.1.26.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.

21.6.1.1.26.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.

21.6.1.1.26.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.

21.6.1.1.26.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

21.6.1.1.26.5. Deve permitir a criação de categorias personalizadas.

21.6.1.1.26.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.

21.6.1.1.26.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.

21.6.1.1.26.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.

21.6.1.1.26.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.

21.6.1.1.26.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;

21.6.1.1.26.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

21.6.1.1.26.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

21.6.1.1.26.13. Criar políticas baseadas na visibilidade e controle de acesso que

permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;

21.6.1.1.26.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

21.6.1.1.26.15. Permitir a criação de categorias de URLs customizadas;

21.6.1.1.26.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;

21.6.1.1.26.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;

21.6.1.1.26.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

21.6.1.1.26.19. Permitir a customização de página de bloqueio;

21.6.1.1.26.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;

21.6.1.1.26.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;

21.6.1.1.26.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

21.6.1.1.26.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;

21.6.1.1.26.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;

21.6.1.1.26.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

21.6.1.1.26.26. Implementar a criação de grupos customizados de usuários no

Firewall, baseado em atributos do LDAP e LDAP/AD;

- 21.6.1.1.26.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 21.6.1.1.26.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 21.6.1.1.26.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 21.6.1.1.26.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 21.6.1.1.26.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 21.6.1.1.26.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 21.6.1.1.26.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 21.6.1.1.26.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 21.6.1.1.26.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 21.6.1.1.26.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 21.6.1.1.26.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 21.6.1.1.26.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 21.6.1.1.26.39. Deve possuir Proxy Explícito e Transparente.
- 21.6.1.1.26.40. Deve implementar roteamento WCCP e ICAP.
- 21.6.1.1.27. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)
 - 21.6.1.1.27.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
 - 21.6.1.1.27.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500

(três mil e quinhentas) ameaças conhecidas.

- 21.6.1.1.27.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 21.6.1.1.27.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 21.6.1.1.27.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 21.6.1.1.27.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 21.6.1.1.27.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 21.6.1.1.27.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 21.6.1.1.27.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 21.6.1.1.27.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 21.6.1.1.27.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 21.6.1.1.27.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 21.6.1.1.27.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 21.6.1.1.27.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 21.6.1.1.27.15. Deve possuir capacidade de remontagem de pacotes para

identificação de ataques.

- 21.6.1.1.27.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 21.6.1.1.27.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 21.6.1.1.27.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 21.6.1.1.27.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 21.6.1.1.27.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 21.6.1.1.27.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 21.6.1.1.27.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 21.6.1.1.27.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 21.6.1.1.27.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 21.6.1.1.27.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 21.6.1.1.27.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 21.6.1.1.27.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 21.6.1.1.27.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

- 21.6.1.1.27.29. Identificar, alertar e bloquear comunicação com botnets;
- 21.6.1.1.27.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 21.6.1.1.27.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 21.6.1.1.27.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 21.6.1.1.27.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 21.6.1.1.27.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 21.6.1.1.27.35. Identificar nos eventos o país de onde partiu a ameaça;
- 21.6.1.1.27.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 21.6.1.1.27.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 21.6.1.1.27.38. Deve possuir alarmes na console de administração.
- 21.6.1.1.27.39. Deve possuir alertas via correio eletrônico.
- 21.6.1.1.27.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 21.6.1.1.27.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 21.6.1.1.27.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 21.6.1.1.27.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);

21.6.1.1.27.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

21.6.1.1.28. FUNCIONALIDADE DE VPN

- 21.6.1.1.28.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
- 21.6.1.1.28.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
- 21.6.1.1.28.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
- 21.6.1.1.28.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
- 21.6.1.1.28.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
- 21.6.1.1.28.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
- 21.6.1.1.28.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
- 21.6.1.1.28.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 21.6.1.1.28.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 21.6.1.1.28.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 21.6.1.1.28.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 21.6.1.1.28.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 21.6.1.1.28.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 21.6.1.1.28.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 21.6.1.1.28.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;

21.6.1.1.28.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.

21.6.1.1.28.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPsec estabelecidos.

21.6.1.1.29. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

21.6.1.1.29.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;

21.6.1.1.29.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;

21.6.1.1.29.3. Atualizar a base de assinaturas de aplicações automaticamente;

21.6.1.1.29.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.

21.6.1.1.29.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

21.6.1.1.29.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;

21.6.1.1.29.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;

21.6.1.1.29.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

21.6.1.1.29.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;

- 21.6.1.1.29.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 21.6.1.1.29.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 21.6.1.1.29.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 21.6.1.1.29.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 21.6.1.1.29.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 21.6.1.1.29.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 21.6.1.1.29.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 21.6.1.1.29.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 21.6.1.1.29.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.

- 21.6.1.1.29.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 21.6.1.1.29.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 21.6.1.1.29.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 21.6.1.1.29.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 21.6.1.1.29.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 21.6.1.1.29.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 21.6.1.1.29.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 21.6.1.1.29.26. Deve permitir criação de padrões de aplicação manualmente.
- 21.6.1.1.29.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 21.6.1.1.29.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 21.6.1.1.29.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 21.6.1.1.29.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;

21.6.1.1.30. FUNCIONALIDADE DE SD-WAN

- 21.6.1.1.30.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
- 21.6.1.1.30.2. O plano de controle e orquestração SD-WAN deve ser local e

operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com monitoramento, orquestração e plano de controle SD-WAN baseados em nuvem.

- 21.6.1.1.30.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
- 21.6.1.1.30.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 21.6.1.1.30.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 21.6.1.1.30.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 21.6.1.1.30.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 21.6.1.1.30.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 21.6.1.1.30.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 21.6.1.1.30.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 21.6.1.1.30.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 21.6.1.1.30.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 21.6.1.1.30.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 21.6.1.1.30.14. Passivo: uso do tráfego real para as medições;

- 21.6.1.1.30.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 21.6.1.1.30.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 21.6.1.1.30.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 21.6.1.1.30.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 21.6.1.1.30.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 21.6.1.1.30.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 21.6.1.1.30.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 21.6.1.1.30.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 21.6.1.1.30.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);

- 21.6.1.1.30.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 21.6.1.1.30.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 21.6.1.1.30.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 21.6.1.1.30.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 21.6.1.1.30.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 21.6.1.1.30.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;
- 21.6.1.1.31. FUNCIONALIDADE DE PROXY DE ACESSO ZTA (ZERO TRUST ACCESS)
 - 21.6.1.1.31.1. Deve sincronizar ZTA Tags da SOLUÇÃO DE ZERO TRUST ACCESS, convertendo-as em objetos de endereço dinâmicos.
 - 21.6.1.1.31.2. As ZTA Tags devem ser utilizáveis em:
 - 21.6.1.1.31.3. Regras ZTA (acesso condicional a aplicações internas).
 - 21.6.1.1.31.4. Firewall Policies (com verificação de tags habilitada).
 - 21.6.1.1.31.5. Inclusão de campos de ZTA Tags nos logs de tráfego.
 - 21.6.1.1.31.6. Atualização Dinâmica de Tags.
 - 21.6.1.1.31.7. Deve permitir proxy reverso (reverse proxy) de aplicações HTTP e HTTPS por meio de VIPs (Virtual IPs) configuráveis, atuando como ponto de acesso seguro entre o cliente e os servidores internos protegidos.

- 21.6.1.1.31.8. Deve ser compatível com mecanismos de autenticação adicional, como SAML, permitindo redirecionamento automático do cliente a portais de autenticação (captive portals) antes do acesso à aplicação interna.
- 21.6.1.1.31.9. Deve permitir funcionamento como proxy de aplicações não-HTTP (TCP Forwarding Access Proxy), encapsulando tráfego TCP dentro de conexões HTTPS estabelecidas entre cliente e gateway, garantindo proteção e controle de acesso baseado em política ZTA.
- 21.6.1.1.31.10. Deve suportar protocolos de aplicação no modelo TCP forwarding, incluindo, mas não se limitando a: RDP, SSH, SMB, FTP, SMTP, SMTPS, IMAP, IMAPS, POP3, POP3S, CIFS e HTTP/S, com possibilidade de inspeção profunda (deep inspection).
- 21.6.1.1.31.11. Deve suportar o proxy de sessões SSH.
- 21.6.1.1.31.12. Deve obter, em tempo real, certificado digital de cliente emitido por autoridade certificadora interna da SOLUÇÃO ZTA (ZTA Certificate Authority), garantindo identidade confiável do endpoint antes do início da sessão.
- 21.6.1.1.31.13. Deve ser capaz de aplicar políticas ZTA com base em múltiplos atributos do endpoint, incluindo postura de segurança, usuário logado, e outras tags atribuídas dinamicamente.
- 21.6.1.1.31.14. Deve manter sincronização contínua com SOLUÇÃO ZTA, recebendo informações de postura de segurança e certificados para autenticação ZTA.

21.6.1.2. TÉCNICO RESIDENTE CENTRO DE OPERAÇÕES DE REDE

- 21.6.1.2.1. A CONTRATADA deve disponibilizar 01 (um) técnicos residentes de operações de rede, que devem ficar alocados no mesmo ambiente do Centro de Operações de Segurança.
- 21.6.1.2.2. Os serviços envolvem a execução de atividades de rotina do Centro de Operações, que devem ser prestados de maneira contínua para apoiar os processos de trabalho e atividades pontuais.
- 21.6.1.2.3. Os serviços envolvem todas as atividades de rotina, configurações, programações, atendimento às demandas apresentadas pelo CONTRATANTE.
- 21.6.1.2.4. Os profissionais estarão à disposição da CONTRATANTE para os serviços continuados em regime de dedicação exclusiva, em dias e horários definidos pelo

gestor do contrato observando-se a carga horária de 44 horas semanais.

- 21.6.1.2.5. A execução do contrato seguirá metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada, a contratante caberá a responsabilidade de definir demandas, bem como realizar o monitoramento qualitativo dos serviços. A contratada deverá disponibilizar um Gerente do Projeto, que deverá supervisionar toda atividade dos profissionais vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidade de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela CONTRATANTE.
- 21.6.1.2.6. O Gerente do Projeto deverá realizar no mínimo uma visita semanal ao CONTRATANTE e estar disponível para reuniões, esclarecimentos e apoio às atividades quando solicitado de Gestor do Contrato.
- 21.6.1.2.7. Os serviços deverão ser realizados nas dependências da CONTRATANTE, utilizando-se de equipamentos e infraestrutura com capacidade operacional.
- 21.6.1.2.8. Os serviços deverão ser realizados por profissionais, detentores de diplomas de nível superior em áreas afins da Tecnologia da Informação, com experiência comprovada mínima de 3 anos, na implantação, operação e suporte de dispositivos de Segurança da Informação, com características similares às apresentadas pela CONTRATANTE.
- 21.6.1.2.9. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.
- 21.6.1.2.10. Os profissionais deverão estudar os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE, para execução das atividades de rotina, não se admitindo, em qualquer hipótese, alegação de desconhecimento dos mesmos;
- 21.6.1.2.11. DISPOSIÇÕES COMPLEMENTARES:
- 21.6.1.2.12. Todos os encargos sociais e seguros em geral, necessários na execução das atividades exercidas pelos profissionais da Contratada, inclusive durante o transporte dos profissionais a serviço da CONTRATANTE, são de responsabilidade exclusiva da Contratada.
- 21.6.1.2.13. A Contratada deverá realizar regularmente os exames de saúde dos seus empregados, na forma da lei, assim como arcar com todas as despesas

decorrentes de transporte, alimentação, inclusive seguro de vida contra o risco de acidentes de trabalho e outras especificadas nos dissídios ou convenções coletivas.

- 21.6.1.2.14. Cada prestador de serviço deverá apresentar-se uniformizado, com fardamento padrão fornecido pela Contratada, portando crachá de identificação.
- 21.6.1.2.15. Manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e recursos humanos para execução completa e eficiente dos serviços objeto deste contrato.
- 21.6.1.2.16. Responder perante a CONTRATANTE pela conduta, frequência, pontualidade e assiduidade de seus empregados e efetuar as substituições daqueles que venham a se ausentar do serviço, por motivo justificado ou não, sem nenhum ônus para o CONTRATANTE, bem como comunicar a CONTRATANTE, antecipadamente, todo e qualquer afastamento, substituição ou inclusão de qualquer um dos seus empregados vinculados à execução do presente contrato.
- 21.6.1.2.17. Zelar pela boa e completa execução dos serviços e facilitar, por todos os meios ao seu alcance, a ampla ação fiscalizadora dos prepostos designados pelo CONTRATANTE, atendendo prontamente às observações e exigências que lhe forem solicitadas.
- 21.6.1.2.18. Arcar com todo e qualquer dano ou prejuízo de qualquer natureza causado à CONTRATANTE e terceiros, por sua culpa, ou em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir o equivalente a todos os danos decorrentes de paralisação ou interrupção dos serviços contratados, exceto quando isto ocorrer por exigência da CONTRATANTE ou ainda por caso fortuito ou força maior, circunstâncias que deverão ser comunicadas no prazo de 48 (quarenta e oito) horas após a sua ocorrência.
- 21.6.1.2.19. Não efetuar despesa, celebrar acordos, fazer declarações ou prestar informações em nome do CONTRATANTE.
- 21.6.1.2.20. Comunicar imediatamente ocorrências de qualquer natureza que impeçam o bom andamento do serviço.

21.6.1.3. PLATAFORMA CENTRALIZADA DE GERENCIAMENTO DE DISPOSITIVOS

- 21.6.1.3.1. A solução deverá ser fornecida na forma de appliance físico ou como solução virtual, compatível com as plataformas VMware, Microsoft Hyper-V e KVM.
- 21.6.1.3.2. No caso de solução virtualizada, caberá à CONTRATANTE a responsabilidade pelo

fornecimento do servidor/hardware, incluindo todos os licenciamentos necessários.

- 21.6.1.3.3. Deverá possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 60 (sessenta) meses.
- 21.6.1.3.4. Deve ser compatível, integrável e do mesmo fabricante da SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW dos itens SOLUÇÃO DE CONECTIVIDADE SEGURA – TIPO 01, TIPO 02, TIPO 03, TIPO 04, TIPO 05, TIPO 06, TIPO 13, TIPO 14, TIPO 15, TIPO 16.
- 21.6.1.3.5. Deve possuir licença para gerenciar de forma centralizada de no mínimo 5.000 dispositivos.
- 21.6.1.3.6. Deve garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo.
- 21.6.1.3.7. Deve possuir definição de perfis de acesso ao console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.
- 21.6.1.3.8. Deve gerar alertas automáticos via e-mail e snmp.
- 21.6.1.3.9. Deve monitorar a performance e Status dos links conectados a Solução de Segurança dos links de Internet.
- 21.6.1.3.10. Deve possibilitar a criação e administração de políticas de firewall, controle de aplicação, sistema prevenção a intrusão (IPS - intrusion prevention system), antivírus, SD-WAN, VPN e de filtro de URL.
- 21.6.1.3.11. Deve permitir usar palavras chaves ou cores para facilitar identificação de regras.
- 21.6.1.3.12. Deve permitir localizar quais regras um objeto (ex. Computador, serviço etc.) Está sendo utilizado.
- 21.6.1.3.13. Deve atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS.
- 21.6.1.3.14. Deve permitir criação de regras que fiquem ativas em horário definido.
- 21.6.1.3.15. Deve permitir criação de regras com data de expiração.
- 21.6.1.3.16. Deve permitir realizar o backup das configurações para permitir o retorno (rollback) de uma configuração salva.
- 21.6.1.3.17. Deve possuir mecanismo de validação das políticas, avisando quando houver

regras que ofusquem ou conflitem com outras (shadowing), ou garantir que esta exigência seja plenamente atendida por meio diverso.

- 21.6.1.3.18. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.
- 21.6.1.3.19. Deve garantir que todos os componentes da SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW dos itens SOLUÇÃO DE CONECTIVIDADE SEGURA - TIPO 01, TIPO 02, TIPO 03, TIPO 04, TIPO 05, TIPO 06, TIPO 13, TIPO 14, TIPO 15, TIPO 16 sejam controlados de forma centralizada, utilizando apenas uma plataforma de gerência.
- 21.6.1.3.20. Deve garantir que os dispositivos de segurança sejam visualizados na operação integrada da rede através de geolocalização, e integrados com uma aplicação de mapas online (google maps, bing maps ou outra equivalente).
- 21.6.1.3.21. Deve possuir um sistema de backup/restauração de todas as configurações da solução de gerência, assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora.
- 21.6.1.3.22. Deve permitir ao administrador transferir os backups para um servidor SFTP.
- 21.6.1.3.23. Deve realizar a função de gerência em um equipamento exclusivo, não exercendo outras funções (como firewall).
- 21.6.1.3.24. Deve garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota, de maneira centralizada.
- 21.6.1.3.25. Deve permitir aos administradores se autenticarem nos servidores de gerência através de contas de usuários locais, de bases externas LDAP e RADIUS.
- 21.6.1.3.26. Deve suportar e realizar a sincronização do relógio interno dos equipamentos da solução via protocolo NTP.
- 21.6.1.3.27. Deve gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas.
- 21.6.1.3.28. Deve permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como licenças, horário do sistema e firmware.
- 21.6.1.3.29. Deve permitir criar os objetos que serão utilizados nas políticas, de forma centralizada.
- 21.6.1.3.30. Deve possuir um assistente integrado ao painel de operações, baseado em inteligência artificial generativa (Assistente de IA), que auxilie na configuração do ambiente, na configuração de funcionalidades de VPN e SD-WAN e na investigação

de problemas no ambiente gerenciado;

- 21.6.1.3.31. O Assistente de IA deve permitir que administradores utilizem comandos em linguagem natural, a fim de facilitar a execução de tarefas;
- 21.6.1.3.32. O Assistente de IA deve interpretar o estado dos dispositivos gerenciados e, em caso de ser encontrado algum problema, recomendar ações corretivas;
- 21.6.1.3.33. O Assistente de IA deve ter a capacidade de criar e revisar scripts de configurações antes de serem aplicados na solução de gerência centralizada;
- 21.6.1.3.34. Caso a solução de gerenciamento não possua assistente de IA nativo, será permitida a composição com soluções e plataformas de IA generativa complementares desde que devidamente licenciadas, integradas e operacionais e atendendo plenamente aos requisitos técnicos exigidos.

21.6.1.4. SOLUÇÃO DE ZERO TRUST ACCESS

- 21.6.1.4.1. Funcionalidades mínimas da Solução de ZTA (Zero Trust Access), de responsabilidade da CONTRATADA:
- 21.6.1.4.2. Deve disponibilizar uma console central do próprio fabricante licenciada para, no mínimo, 5.000 (cinco mil) agentes ZTA durante a vigência contratual a ser disponibilizada localmente em máquina virtual compatível com VMWare ESXi ou HyperV ou KVM de responsabilidade da CONTRATANTE ou em nuvem do próprio fabricante;
- 21.6.1.4.3. Garante acesso seguro a aplicativos hospedados em qualquer lugar, quer os usuários estejam trabalhando remotamente ou no ambiente corporativo. De acordo com o conceito da confiança zero (Zero Trust), usuários e dispositivos são considerados confiáveis somente depois de terem sido verificados.
- 21.6.1.4.4. A solução de ZTA deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas;
- 21.6.1.4.5. Deve ser compatível e do mesmo fabricante da solução de firewall proposta nos ITENS SOLUÇÃO DE CONECTIVIDADE SEGURA 01, 02, 03, 04, 05, 06, 13, 14, 15, 16;
- 21.6.1.4.6. A solução de ZTA deve prover um método de controlar o acesso identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust;
- 21.6.1.4.7. A solução de ZTA deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático

para cada sessão;

- 21.6.1.4.8. A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal Web a ser acessado por cada usuário;
- 21.6.1.4.9. O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante;
- 21.6.1.4.10. O agente de ZTA deve ser compatível com no mínimo com Microsoft Windows 11 (64 bits);
- 21.6.1.4.11. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.3;
- 21.6.1.4.12. A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único pelo agente e deverá ainda ser compartilhado com o proxy de acesso;
- 21.6.1.4.13. Deve ser possível revogar o certificado de um agente por meio da console central;
- 21.6.1.4.14. O certificado emitido deve ser utilizado no processo de autenticação via ZTA para identificar o dispositivo do usuário final junto ao proxy de acesso;
- 21.6.1.4.15. No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados estejam diferentes, o acesso deverá ser bloqueado por padrão;
- 21.6.1.4.16. Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional;
- 21.6.1.4.17. A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até cinco dias anteriores ao ocorrido;
- 21.6.1.4.18. Deve ser possível determinar para quais funcionalidades o log deve estar habilitado e permitir que esses dados sejam enviados para a console central;
- 21.6.1.4.19. Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, debug;
- 21.6.1.4.20. Deve ser possível exportar os logs diretamente a nível de agente;
- 21.6.1.4.21. Deve ser possível exigir uma senha para desconectar o agente da console central;
- 21.6.1.4.22. Deve existir a possibilidade de restringir o usuário de realizar backup da

configuração do agente;

- 21.6.1.4.23. Deve ser possível evitar que o usuário realize um shutdown do agente após estar registrado à console central;
- 21.6.1.4.24. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de existente na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 21.6.1.4.25. O agente deve permitir a configuração local via XML (eXtensible Markup Language);
- 21.6.1.4.26. Deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central;
- 21.6.1.4.27. Este convite deve gerar um código a ser inserido no passo de registro do agente e deve ser possível ainda adicionar um passo de verificação da autenticação do usuário, podendo associar a autenticação via base de dados local, LDAP e SAML;
- 21.6.1.4.28. Deverá ser possível enviar uma notificação por e-mail contendo o código de registro para os usuários finais informados, bem como um link para download do instalador do agente;
- 21.6.1.4.29. Deve ser possível especificar a validade do código de registro;
- 21.6.1.4.30. A console central de agentes deve dispor de métodos para determinar se um usuário está on-net ou off-net, ou seja, dentro ou fora da rede corporativa. Deve ser possível ainda criar perfis de configurações distintos para os usuários on-net e off-net.
- 21.6.1.4.31. Deve ser possível agrupar agentes em grupos;
- 21.6.1.4.32. Deve ser possível atribuir grupos de agentes a perfis de políticas específicos;
- 21.6.1.4.33. Deve ser possível atribuir um nível de prioridade a um perfil de política visando priorizar qual política será utilizada caso um grupo de agentes esteja associado a mais de um perfil de política;
- 21.6.1.4.34. A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, informações de rede/endereço IP, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede, detalhes do hardware como modelo do dispositivo, fabricante. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão do agente está em uso em um

respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTA;

- 21.6.1.4.35. O proxy de acesso ZTA deve atuar como proxy reverso para aplicações baseadas em HTTP, HTTPS, RDP, SMB, CIFS, SSH, SMTP, SMTPS, IMAP, IMAPS, POP3 e POP3S;
- 21.6.1.4.36. Para aplicações HTTP e HTTPS deve ser possível realizar um balanceamento de carga entre os servidores cadastrados usando algoritmos como round robin, por peso, ou baseado em disponibilidade do servidor;
- 21.6.1.4.37. Para regras de encaminhamento de tráfego TCP, deve ser possível vincular o servidor com um FQDN;
- 21.6.1.4.38. Deve ser possível definir um pool de IPs no proxy de acesso como IPs de origem para comunicação interna com as aplicações privadas;
- 21.6.1.4.39. A console central deve permitir mapear as regras de destinos de ZTA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia;
- 21.6.1.4.40. Deve permitir criação de regras de conformidade que avaliem a postura do dispositivo e auxiliem o administrador no controle de acesso aos recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas;
- 21.6.1.4.41. As regras de conformidade devem gerar tags que são sincronizadas entre os elementos da solução de ZTA visando controlar a postura de um determinado endpoint diretamente no proxy de acesso;
- 21.6.1.4.42. Deve distribuir e sincronizar tags Zero Trust para os dispositivos dos ITENS SOLUÇÃO DE CONECTIVIDADE SEGURA TIPO 01, 02, 03, 04, 06, 08, 13, 14, 15, 16 para que as mesmas possam ser utilizadas em regras e políticas de segurança avançadas de controle de acesso;
- 21.6.1.4.43. A postura deve ser monitorada continuamente para que, caso ocorra uma alteração, o proxy de acesso termine e passe a bloquear a conexão em desacordo com as regras de compliance definidas;
- 21.6.1.4.44. Deve ser possível construir tags com verificações no endpoint, as quais podem variar de acordo com o suporte ao sistema operacional, tais como se o endpoint está logado no domínio, versão do sistema operacional, chave de registro, processo, nível de vulnerabilidade, CVEs, arquivos existentes em um caminho

específico e até mesmo se o antivírus está instalado e sendo executado, além de ser possível validar se as assinaturas estão atualizadas;

- 21.6.1.4.45. A console central deve permitir exportar e importar tags entre sistemas diferentes por meio de um arquivo JSON;
- 21.6.1.4.46. Deve ser possível verificar quais endpoints estão associadas com cada tag;
- 21.6.1.4.47. Deve ser possível criar regras no proxy de acesso determinando se um dispositivo necessita estar de acordo com uma ou mais de uma tag simultaneamente, caso a política possua vínculo com diversas tags;
- 21.6.1.4.48. Deve ser possível criar regras no proxy de acesso vinculando interface de origem, IP de origem, IP de destino, servidor ZTA, tag ZTA, grupo de usuários ou usuário;
- 21.6.1.4.49. Para validação da autenticação dos usuários em conjunto com as regras de proxy de acesso, a solução deve suportar SAML, LDAP, Radius ou base de dados local;
- 21.6.1.4.50. A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional;
- 21.6.1.4.51. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente;
- 21.6.1.4.52. Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos;
- 21.6.1.4.53. Caso não seja possível aplicar um patch automático para corrigir uma vulnerabilidade, requerendo assim um patch manual, deve ser possível excluir essa aplicação da verificação de compliance;
- 21.6.1.4.54. Deve ser possível excluir determinadas aplicações da verificação de compliance e até mesmo desabilitar o patch automático;
- 21.6.1.4.55. O agente deve dispor de um sistema de notificação do tipo pop-up visando alertar o usuário;
- 21.6.1.4.56. Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, severidade, bem como o CVE correspondente;
- 21.6.1.4.57. Deve suportar a criação de várias versões de pacotes de instalação;
- 21.6.1.4.58. As vulnerabilidades encontradas devem ser exibidas diretamente no agente com um link para análise de mais detalhes, englobando nome da vulnerabilidade, severidade, produtos afetados, CVE IDs, descrição, informação do fabricante do

software e, quando disponível, link para download do patch no site público do fabricante do software;

- 21.6.1.4.59. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas, bem como disponibilizar ainda a possibilidade de aplicar a remediação imediatamente;
- 21.6.1.4.60. Deve possuir módulo para execução de filtro web a nível de endpoint mediante uso do agente local, realizando a filtragem diretamente no endpoint, podendo ainda ser possível bloquear, permitir, alertar ou monitorar o tráfego web com base na categoria de URL ou filtro de URL customizado;
- 21.6.1.4.61. O agente deve realizar consultas online ao centro de inteligência do próprio fabricante para determinar a categoria de uma determinada URL visando aplicar o controle de acesso à Internet;
- 21.6.1.4.62. Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar;
- 21.6.1.4.63. O agente para Windows deve permitir inspeção de tráfego HTTPS mediante instalação de plugin disponibilizado pelo mesmo fabricante do agente, o qual deve ser compatível com Google Chrome, Mozilla Firefox e Microsoft Edge;
- 21.6.1.4.64. Deve ser possível verificar as violações de filtro web diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário;
- 21.6.1.4.65. Deve ser possível determinar quando o filtro web entrará em ação no agente, se ele deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa;
- 21.6.1.4.66. Deve ser possível configurar o proxy de acesso para atuar como CASB (Cloud Access Security Broker) em linha, inline do inglês, visando controlar o acesso a aplicações SaaS;
- 21.6.1.4.67. O proxy de acesso deve manter uma base de aplicações dinâmica, a qual deve ser compartilhada pelo centro de inteligência do fabricante da solução.
- 21.6.1.4.68. O agente deverá ter a capacidade de inspecionar arquivos executáveis, bibliotecas e drivers quanto a vírus.
- 21.6.1.4.69. O agente deverá ser capaz de verificar atualizações de assinatura automaticamente;
- 21.6.1.4.70. O agente deverá ser capaz de enviar arquivos para inspeção nos sistemas

Sandboxing do mesmo fabricante;

- 21.6.1.4.71. O agente deverá ser capaz de bloquear os canais de comunicação usados por hackers ou atacantes;
- 21.6.1.4.72. O agente deverá permitir que o usuário inicie uma verificação sob demanda;
- 21.6.1.4.73. O agente deverá permitir que a verificação de vírus seja iniciada automaticamente regularmente;
- 21.6.1.4.74. O agente deverá permitir a visualização dos arquivos em quarentena
- 21.6.1.4.75. Deverá permitir a configuração do perfil antivírus a partir do console central do mesmo fabricante;
- 21.6.1.4.76. Deverá ter uma solução de proteção contra malware baseada em nuvem. Essa proteção deve ser capaz de gerar uma soma de verificação do arquivo acessado e consultar a nuvem se essa soma de verificação corresponder a uma nova ameaça;
- 21.6.1.4.77. Deverá ser capaz de enviar arquivos para uma solução de proteção avançada de ameaças (ATP) (ou sandboxing) antes de ser acessado;
- 21.6.1.4.78. Deverá ser capaz de bloquear o acesso ao arquivo até que o sandbox dê um veredicto;
- 21.6.1.4.79. Caso um arquivo seja marcado como malicioso pela Sandbox, o mesmo deverá ser mantido em quarentena;

21.6.1.5. TÉCNICO RESIDENTE CENTRO DE OPERAÇÕES DE SEGURANÇA

- 21.6.1.5.1. A CONTRATADA deve disponibilizar 01 (um) técnicos residentes de operações de cibersegurança, que devem ficar alocados no mesmo ambiente do Centro de Operações de Segurança
- 21.6.1.5.2. Os serviços envolvem a execução de atividades de rotina do Centro de Operações de Segurança da e devem ser prestados de maneira contínua para apoiar os processos de trabalho e atividades pontuais.
- 21.6.1.5.3. Os serviços envolvem todas as atividades de rotina, configurações, programações, atendimento às demandas apresentadas pelo CONTRATANTE.
- 21.6.1.5.4. Os profissionais estarão à disposição da CONTRATANTE para os serviços continuados em regime de dedicação exclusiva, em dias e horários definidos pelo gestor do contrato observando-se a carga horária de 44 horas semanais.
- 21.6.1.5.5. A execução do contrato seguirá metodologia de trabalho baseado no conceito de

Delegação de Responsabilidade Supervisionada, a contratante caberá a responsabilidade de definir demandas, bem como realizar o monitoramento qualitativo dos serviços. A contratada deverá disponibilizar um Gerente do Projeto, que deverá supervisionar toda atividade dos profissionais vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidade de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela CONTRATANTE.

- 21.6.1.5.6. O Gerente do Projeto deverá realizar no mínimo uma visita semanal ao CONTRATANTE e estar disponível para reuniões, esclarecimentos e apoio às atividades quando solicitado de Gestor do Contrato.
- 21.6.1.5.7. Os serviços deverão ser realizados nas dependências da CONTRATANTE, utilizando-se de equipamentos e infraestrutura com capacidade operacional.
- 21.6.1.5.8. Os serviços deverão ser realizados por profissionais, detentores de diplomas de nível superior em áreas afins da Tecnologia da Informação, com experiência comprovada mínima de 3 anos, na implantação, operação e suporte de dispositivos de Segurança da Informação, com características similares às apresentadas pela CONTRATANTE.
- 21.6.1.5.9. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.
- 21.6.1.5.10. Os profissionais deverão estudar os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE, para execução das atividades de rotina, não se admitindo, em qualquer hipótese, alegação de desconhecimento dos mesmos.
- 21.6.1.5.11. DISPOSIÇÕES COMPLEMENTARES:
 - 21.6.1.5.11.1. Todos os encargos sociais e seguros em geral, necessários na execução das atividades exercidas pelos profissionais da Contratada, inclusive durante o transporte dos profissionais a serviço da CONTRATANTE, são de responsabilidade exclusiva da Contratada.
 - 21.6.1.5.11.2. A Contratada deverá realizar regularmente os exames de saúde dos seus empregados, na forma da lei, assim como arcar com todas as despesas decorrentes de transporte, alimentação, inclusive seguro de vida contra o risco de acidentes de trabalho e outras especificadas nos dissídios

ou convenções coletivas.

21.6.1.5.11.3. Cada prestador de serviço deverá apresentar-se uniformizado, com fardamento padrão fornecido pela Contratada, portando crachá de identificação.

21.6.1.5.11.4. Manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e recursos humanos para execução completa e eficiente dos serviços objeto deste contrato.

21.6.1.5.11.5. Responder perante a CONTRATANTE pela conduta, frequência, pontualidade e assiduidade de seus empregados e efetuar as substituições daqueles que venham a se ausentar do serviço, por motivo justificado ou não, sem nenhum ônus para o CONTRATANTE, bem como comunicar a CONTRATANTE, antecipadamente, todo e qualquer afastamento, substituição ou inclusão de qualquer um dos seus empregados vinculados à execução do presente contrato.

21.6.1.5.11.6. Zelar pela boa e completa execução dos serviços e facilitar, por todos os meios ao seu alcance, a ampla ação fiscalizadora dos prepostos designados pelo CONTRATANTE, atendendo prontamente às observações e exigências que lhe forem solicitadas.

21.6.1.5.11.7. Arcar com todo e qualquer dano ou prejuízo de qualquer natureza causado à CONTRATANTE e terceiros, por sua culpa, ou em consequência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir o equivalente a todos os danos decorrentes de paralisação ou interrupção dos serviços contratados, exceto quando isto ocorrer por exigência da CONTRATANTE ou ainda por caso fortuito ou força maior, circunstâncias que deverão ser comunicadas no prazo de 48 (quarenta e oito) horas após a sua ocorrência.

21.6.1.5.11.8. Não efetuar despesa, celebrar acordos, fazer declarações ou prestar informações em nome do CONTRATANTE.

21.6.1.5.11.9. Comunicar imediatamente ocorrências de qualquer natureza que impeçam o bom andamento do serviço.

21.7.IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

21.7.1.1. A infraestrutura do Centro de Monitoramento e Controle será responsável por gerenciar e integrar todas as soluções distribuídas nas unidades governamentais, conforme

estabelecido neste Termo de Referência.

- 21.7.1.2. Todas as Soluções de Conectividade Segura implantadas deverão ser plenamente compatíveis e gerenciáveis pelo conjunto plataforma centralizada de gerenciamento de dispositivos e solução de de relatório de logs, garantindo visibilidade, controle e integração de ponta a ponta.
- 21.7.1.3. A solução deverá assegurar um gerenciamento, seguro e coeso da rede governo, promovendo maior eficiência na administração da conectividade e da segurança da informação, além de permitir respostas rápidas a incidentes e tomada de decisão com base em dados confiáveis.
- 21.7.1.4. A contratada deve realizar a instalação de todos os componentes previstos para o Centro de Monitoramento e Controle, garantindo conectividade segura e controle de tráfego.
- 21.7.1.5. Todos os componentes/equipamentos integrantes desta solução deverão ser alocados em local a definir pela PRODEB, garantindo:
- 21.7.1.6. Organização e proteção adequada dos ativos de rede e segurança.
- 21.7.1.7. Ambiente climatizado e protegido contra falhas energéticas.
- 21.7.1.8. A Contratada deverá fornecer todos os patch-cords e cordões ópticos adequados para a conexão dos equipamentos, garantindo conformidade com a topologia estabelecida.
- 21.7.1.9. A Contratante será responsável pelo fornecimento e adequação da infraestrutura elétrica necessária para o funcionamento do Core de Rede, garantindo a alimentação adequada e contínua de todos os componentes da solução.
- 21.7.2. SERVIÇOS DE IMPLANTAÇÃO - CONDIÇÕES GERAIS PARA TODOS OS SERVIÇOS DE IMPLANTAÇÃO
 - 21.7.2.1. Para todos os serviços de implantação, a CONTRATADA deverá cumprir os seguintes requisitos:
 - 21.7.2.2. Início da implantação em até 30 (trinta) dias após aprovação do cronograma executivo pela CONTRATANTE.
 - 21.7.2.3. Execução dos serviços sem ônus adicional para a CONTRATANTE.
 - 21.7.2.4. Disponibilização de equipe técnica qualificada, com certificações compatíveis com os componentes da solução.
 - 21.7.2.5. Utilização de ferramentas, materiais, EPIS e procedimentos de segurança adequados.
 - 21.7.2.6. Execução conforme normas técnicas e de segurança vigentes, sem causar riscos ou interferência nas atividades;
 - 21.7.2.7. Conclusão da implantação mediante testes operacionais bem-sucedidos, acompanhados

pelo responsável técnico da CONTRATANTE.

21.7.2.8. Fornecimento de relatórios de progresso periódicos e recomendações técnicas, sempre que necessário.

21.7.3. IMPLANTAÇÃO DA SOLUÇÃO DE OPERAÇÃO, GERENCIAMENTO E MONITORAMENTO CENTRAL

21.7.3.1. A implantação do Solução de Operação, Gerenciamento e Monitoramento Central será realizada em conformidade com as diretrizes estabelecidas pela CONTRATANTE, garantindo que toda a infraestrutura seja configurada e ativada conforme as melhores práticas de segurança, conectividade e gerenciamento.

21.7.3.2. ESCOPO DA IMPLANTAÇÃO

21.7.3.2.1. A implantação do Centro Monitoramento incluirá os seguintes serviços:

21.7.3.2.2. Planejamento e definição da arquitetura lógica e física do ambiente, assegurando aderência aos requisitos técnicos e operacionais.

21.7.3.2.3. Instalação e configuração da infraestrutura de segurança, conectividade e gerenciamento centralizado.

21.7.3.2.4. Configuração dos dispositivos de segurança cibernética NGFW em HA (02 dispositivos), garantindo alta disponibilidade e proteção avançada.

21.7.3.2.5. Integração e validação da Solução de Gerenciamento Centralizado e da Solução de Relatoria de Logs, assegurando compatibilidade com as soluções prevista neste termo.

21.7.3.2.6. Admissão dos links de internet existentes no local, garantindo conectividade confiável e redundante.

21.7.3.2.7. Execução de testes operacionais e validação conjunta com a CONTRATANTE, assegurando o funcionamento adequado de toda a solução.

21.7.3.2.8. Elaboração de documentação técnica "as built", contendo todos os registros de configuração e ajustes finais.

21.7.4. RESPONSABILIDADES DA CONTRATADA

21.7.4.1. A CONTRATADA será responsável por:

21.7.4.2. Disponibilizar todos os recursos necessários para a implantação, incluindo hardware, software e equipe técnica qualificada.

21.7.4.3. Garantir que a instalação seja realizada nos locais designados pela CONTRATANTE, conforme a topologia definida.

21.7.4.4. Fornecer os patch-cords e cordões ópticos necessários para interligação dos

equipamentos.

21.7.4.5. Atuar em conformidade com as normas técnicas e de segurança vigentes.

21.7.4.6. Realizar a ativação da solução e validar o funcionamento por meio de testes operacionais.

21.7.4.7. Designar um responsável técnico para atuar como ponto focal para suporte, escalonamento junto ao fabricante e coordenação do serviço.

21.7.4.8. Garantir que o projeto respeite prazos e processos de homologação, seguindo metodologias de melhores práticas.

21.7.4.9. IMPLANTAÇÃO DAS SOLUÇÕES DE CONECTIVIDADE SEGURA - TIPOS I a VI e TIPOS XIII a XV

21.7.4.10. A implantação dos SOLUÇÕES DE CONECTIVIDADE SEGURA - TIPOS I a VI e TIPOS XIII a XV será conduzida de forma padronizada, garantindo a integração com a infraestrutura do Centro De Monitoramento.

21.7.5. ESCOPO DA IMPLANTAÇÃO

21.7.5.1. A implantação de cada Solução de Conectividade Segura incluirá:

21.7.5.2. Instalação, configuração e adequação necessária a infraestrutura dos componentes existentes na Solução.

21.7.5.3. Integração completa com a Plataforma Centralizada de Gerenciamento e a Plataforma de Relatoria de Logs.

21.7.5.4. Execução de testes de validação técnica e otimização.

21.7.5.5. Treinamento hands-on operacional básico da equipe local da CONTRATANTE.

21.7.6. RESPONSABILIDADES DA CONTRATADA

21.7.6.1. A CONTRATADA será responsável por:

21.7.6.2. Garantir a correta instalação física e lógica dos equipamentos.

21.7.6.3. Executar a validação do funcionamento dos dispositivos em conjunto com a CONTRATANTE.

21.7.6.4. Observar as normas de segurança do trabalho durante toda a execução do serviço.

21.7.6.5. Fornecer suporte técnico especializado para troubleshooting e análise de vulnerabilidades.

21.8. REQUISITOS DE TREINAMENTO

21.8.1.1. A CONTRATADA deverá fornecer treinamento técnico presencial (in loco), a ser realizado nas dependências da CONTRATANTE, sobre as soluções "SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW", "PLATAFORMA CENTRALIZADA DE GERENCIAMENTO DE

DISPOSITIVOS” e “SOLUÇÃO DE ZERO TRUST ACCESS” contempladas neste item, contemplando 8 (oito) participantes, com foco em administração, operação, monitoramento e segurança das soluções. O treinamento deverá ser realizado apenas na primeira contratação do item, não sendo necessário a repetição das demais contratações.

21.8.1.2. TREINAMENTO PARA SOLUÇÃO FIREWALL DE PRÓXIMA GERAÇÃO NGFW

- 21.8.1.2.1. A carga horária mínima deverá ser compatível com o conteúdo programático descrito neste item, não sendo inferior a 12 (doze) horas, distribuídas conforme cronograma previamente aprovado pela CONTRATANTE;
- 21.8.1.2.2. As aulas deverão combinar conteúdo teórico e atividades práticas (hands-on), utilizando a própria infraestrutura da CONTRATANTE sempre que possível.
- 21.8.1.2.3. O treinamento deverá abranger, no mínimo, os seguintes tópicos:
- 21.8.1.2.4. Configuração de redes;
- 21.8.1.2.5. Administração via interface gráfica (GUI) e linha de comando (CLI);
- 21.8.1.2.6. Métodos de registro e licenciamento do dispositivo;
- 21.8.1.2.7. Visualização, pesquisa e análise de logs no NGFW e em ferramenta de análise centralizada (quando aplicável);
- 21.8.1.2.8. Diagnósticos e Troubleshooting;
- 21.8.1.2.9. Políticas de Firewall;
- 21.8.1.2.10. Roteamento (rotas estáticas, redundância e balanceamento);
- 21.8.1.2.11. Integração com servidores LDAP e RADIUS;
- 21.8.1.2.12. Monitoramento de usuários autenticados;
- 21.8.1.2.13. Funções de criptografia e inspeção SSL;
- 21.8.1.2.14. Perfis de Segurança: Antivirus, Web Filter, IPS, Controle de Aplicação;
- 21.8.1.2.15. Configuração de VPN IPsec;
- 21.8.1.2.16. Configurações de SD-WAN;
- 21.8.1.2.17. High Availability (HA);
- 21.8.1.2.18. A CONTRATADA deverá fornecer material didático em formato digital, em língua portuguesa ou inglesa;

21.8.1.3. TREINAMENTO PARA PLATAFORMA CENTRALIZADA DE GERENCIAMENTO DE DISPOSITIVOS

- 21.8.1.3.1. A carga horária mínima deverá ser compatível com o conteúdo programático descrito neste item, não sendo inferior a 8 (oito) horas, distribuídas conforme cronograma previamente aprovado pela CONTRATANTE;
- 21.8.1.3.2. O treinamento deverá contemplar atividades teóricas e práticas (hands-on), preferencialmente utilizando o ambiente real ou de homologação da CONTRATANTE;
- 21.8.1.3.3. O treinamento deverá abranger, no mínimo, os seguintes tópicos:
- 21.8.1.3.4. Introdução e Configuração Inicial;
- 21.8.1.3.5. Conceitos e funcionalidades principais da solução de gerenciamento centralizado;
- 21.8.1.3.6. Arquitetura, requisitos de implantação e primeiros acessos;
- 21.8.1.3.7. Configuração inicial do sistema;
- 21.8.1.3.8. Administração e Gestão;
- 21.8.1.3.9. Administração de usuários, perfis e permissões;
- 21.8.1.3.10. Boas práticas de governança e segregação administrativa;
- 21.8.1.3.11. Registro e Gerenciamento de Dispositivos;
- 21.8.1.3.12. Histórico de revisões e controle de versões de configuração;
- 21.8.1.3.13. Configuração em Nível de Dispositivo;
- 21.8.1.3.14. Implantação e gerenciamento de configurações individuais;
- 21.8.1.3.15. Uso de modelos (templates) para padronização de parâmetros em múltiplos dispositivos;
- 21.8.1.3.16. Instalação e validação de alterações em larga escala;
- 21.8.1.3.17. Políticas e Objetos;
- 21.8.1.3.18. Criação e gerenciamento centralizado de políticas de segurança;
- 21.8.1.3.19. Aplicação de pacotes de políticas em múltiplos dispositivos ou grupos;
- 21.8.1.3.20. Criação e uso de domínios administrativos para múltiplos ambientes ou clientes;
- 21.8.1.3.21. Administração centralizada de ambientes distribuídos
- 21.8.1.3.22. Diagnóstico e Solução de Problemas;
- 21.8.1.3.23. Diagnóstico de falhas de importação, sincronização e instalação de políticas;
- 21.8.1.3.24. Ferramentas de troubleshooting disponíveis na solução;
- 21.8.1.3.25. Gerenciamento centralizada de firmware e atualizações de dispositivos suportados;
- 21.8.1.3.26. Opções de alta disponibilidade, backup e recuperação da solução;
- 21.8.1.3.27. Distribuição local de atualizações de segurança e inteligência de ameaças;

21.8.1.3.28. A CONTRATADA deverá fornecer material didático em formato digital, em língua portuguesa ou inglesa;

21.8.1.4. TREINAMENTO PARA SOLUÇÃO DE ZERO TRUST ACCESS

- 21.8.1.4.1. A carga horária mínima deverá ser compatível com o conteúdo programático descrito neste item, não sendo inferior a 8 (oito) horas, distribuídas conforme cronograma previamente aprovado pela CONTRATANTE;
- 21.8.1.4.2. O treinamento deverá contemplar atividades teóricas e práticas (hands-on), preferencialmente utilizando o ambiente real ou de homologação da CONTRATANTE;
- 21.8.1.4.3. Segurança de Endpoints e Conceitos de Zero Trust Access;
- 21.8.1.4.4. Papel da segurança de endpoints na arquitetura Zero Trust Access;
- 21.8.1.4.5. Componentes da solução de gerenciamento e proteção de endpoints;
- 21.8.1.4.6. Administração do sistema de gerenciamento central de endpoints;
- 21.8.1.4.7. Perfis de acesso, usuários administrativos e permissões;
- 21.8.1.4.8. Implantação do Agente de Endpoint;
- 21.8.1.4.9. Instalação do agente de endpoint em diferentes sistemas operacionais;
- 21.8.1.4.10. Identificação de funcionalidades, recursos e configurações do agente;
- 21.8.1.4.11. Métodos de distribuição e implantação em larga escala;
- 21.8.1.4.12. Provisionamento de endpoints a partir do gerenciador central;
- 21.8.1.4.13. Criação e aplicação de políticas de endpoints;
- 21.8.1.4.14. Configuração avançada de perfis de segurança e conformidade;
- 21.8.1.4.15. Integração do endpoint com o mecanismo de controle de acesso;
- 21.8.1.4.16. Configuração de políticas de acesso baseadas em identidade, contexto e postura do dispositivo;
- 21.8.1.4.17. Implantação da Solução ZTA;
- 21.8.1.4.18. Publicação e proteção de aplicações internas e remotas;
- 21.8.1.4.19. Controle de acesso por regras de conformidade;
- 21.8.1.4.20. Uso de tags, atributos e validações de postura do endpoints;
- 21.8.1.4.21. Resposta a Incidentes de Segurança;
- 21.8.1.4.22. Detecção e tratamento de incidentes relacionados a endpoints;
- 21.8.1.4.23. Diagnóstico e Solução de Problemas;
- 21.8.1.4.24. Ferramentas de diagnóstico do agente e do gerenciador central;
- 21.8.1.4.25. Análise e resolução de falhas de comunicação, políticas e acesso;

21.8.1.4.26. Boas práticas de troubleshooting em ambientes Zero Trust;

21.8.1.4.27. A CONTRATADA deverá fornecer material didático em formato digital, preferencialmente em língua portuguesa, admitindo-se inglês;

22.LOTE 01 - ITEM 22 - SOLUÇÃO DE RELATORIA DE LOGS TIPO 01

22.1.CARACTERISTICAS DO EQUIPAMENTO

22.1.1. Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização: VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer, no caso de solução virtualizada a responsabilidade pelo fornecimento do servidor/hardware e plataformas de virtualização necessária, será da CONTRATANTE.

22.1.2. Deverá possuir a capacidade de receber pelo menos 2.000 (dois mil) GB de logs dia, além de atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 60 (sessenta) meses

22.1.3. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração.

22.2.REQUISITOS MINIMOS DE FUNCIONALIDADES

22.2.1. Deverá suportar o acesso via SSH ou WEB (HTTPS) para gerenciamento de soluções. Sendo que o gerenciamento administrativo da solução (configuração de Usuários / relatórios) deve ser realizado através de WEB ou GUI. O acesso SSH deve se dar mais para gerir problemas de hardwares e/ou alterações a nível CLI, para alterações no modo de processamento de pacotes e CPU's e troubleshooting.

22.2.2. Deverá possuir comunicação e autenticação criptografada com usuário e senha na interface gráfica (GUI) e via linha de comando no console de gerenciamento.

22.2.3. Deverá permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento.

22.2.4. Deverá suportar SNMP versão 2 e 3.

22.2.5. Deverá permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.

22.2.6. Deverá permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.

22.2.7. Deverá permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH.

- 22.2.8. Deverá possuir autenticação de usuários para acesso à plataforma via LDAP
- 22.2.9. Deverá possuir autenticação de usuários para acesso à plataforma via RADIUS
- 22.2.10. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico.
- 22.2.11. Deverá possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas.
- 22.2.12. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de gráfico
- 22.2.13. Deverá possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.
- 22.2.14. Deverá possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.
- 22.2.15. Deverá possuir visualização da quantidade de logs enviados de cada dispositivo monitorado.
- 22.2.16. Deverá possuir mecanismos de apagamento automático para logs antigos.
- 22.2.17. Deverá permitir importação e exportação de relatórios.
- 22.2.18. Deverá ter a capacidade de criar relatórios no formato HTML.
- 22.2.19. Deverá ter a capacidade de criar relatórios em formato PDF.
- 22.2.20. Deverá ter a capacidade de criar relatórios no formato XML.
- 22.2.21. Deverá permitir exportar os logs no formato CSV.
- 22.2.22. Deverá gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.
- 22.2.23. Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.
- 22.2.24. Deverá ter relatórios predefinidos.
- 22.2.25. Deverá poder enviar automaticamente os logs para um servidor FTP externo para a solução.
- 22.2.26. Deverá permitir a duplicação de relatórios existentes, deve ser possível para edição posterior.
- 22.2.27. Deverá ter a capacidade de personalizar a capa dos relatórios obtidos.
- 22.2.28. Deverá permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.

- 22.2.29. Deverá ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas.
- 22.2.30. Deverá ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real.
- 22.2.31. Deverá permitir que os arquivos de log sejam baixados da plataforma para uso externo.
- 22.2.32. Deverá ter a capacidade de gerar e enviar relatórios periódicos automaticamente.
- 22.2.33. Deverá permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.
- 22.2.34. Deverá permitir o envio por e-mail relatórios automaticamente.
- 22.2.35. Deverá permitir que o relatório seja enviado por e-mail ao destinatário específico.
- 22.2.36. Deverá permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.
- 22.2.37. Deverá exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.
- 22.2.38. Deverá permitir o uso de filtros nos relatórios.
- 22.2.39. Deverá permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.
- 22.2.40. Deverá permitir especificar o idioma dos relatórios criados
- 22.2.41. Deverá gerar alertas automáticos por e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.
- 22.2.42. Deverá permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.
- 22.2.43. Deverá ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.
- 22.2.44. Deverá possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros.
- 22.2.45. Deverá ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.
- 22.2.46. Deverá importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.
- 22.2.47. Deverá ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.
- 22.2.48. Deverá fornecer as informações da quantidade de logs armazenados e as estatísticas do

tempo restante armazenado.

- 22.2.49. Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.
- 22.2.50. Deverá permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos
- 22.2.51. Deverá permitir visualizar em tempo real os logs recebidos.
- 22.2.52. Deverá permitir o encaminhamento de log no formato syslog.
- 22.2.53. Deverá permitir o encaminhamento de log no formato CEF (Common Event Format).
- 22.2.54. Deverá gerar alertas de eventos a partir de logs recebidos.
- 22.2.55. Deverá permitir a criação de incidentes a partir de alertas de eventos para o terminal.
- 22.2.56. Suportar o padrão SAML ou LDAP ou RADIUS para autenticação do usuário administrador.

22.3.FUNCIONALIDADES DE RELATÓRIOS DE FIREWALL

- 22.3.1. Deverá possuir relatório de conformidade com o PCI DSS.
- 22.3.2. Deverá possuir um relatório de uso do aplicativo SaaS.
- 22.3.3. Deverá possuir um relatório de prevenção de perda de dados (DLP).
- 22.3.4. Deverá possuir um relatório de VPN.
- 22.3.5. Deverá possuir um relatório IPS (Intruder Prevention System).
- 22.3.6. Deverá possuir um relatório de reputação do cliente.
- 22.3.7. Deverá possuir um relatório de análise de segurança do usuário.
- 22.3.8. Deverá possuir um relatório de análise de ameaças cibernéticas.
- 22.3.9. Deverá possuir um breve relatório resumido diário de eventos e incidentes de segurança.
- 22.3.10. Deverá possuir um relatório de tráfego DNS.
- 22.3.11. Deverá possuir um relatório de tráfego de e-mail.
- 22.3.12. Deverá possuir um relatório dos 10 principais aplicativos usados na rede.
- 22.3.13. Deverá possuir um relatório dos 10 principais sites usados na rede.
- 22.3.14. Deverá possuir um relatório de uso de mídia social.

23.LOTE 01 - ITEM 23 - SOLUÇÃO DE RELATORIA DE LOGS TIPO 02

23.1.CARACTERISTICAS DO EQUIPAMENTO

- 23.1.1. Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização: VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer, no caso

de solução virtualizada a responsabilidade pelo fornecimento do servidor/hardware e plataformas de virtualização necessária, será da CONTRATANTE.

23.1.2. Deverá possuir a capacidade de receber pelo menos 5 GB de logs dia, além de atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 60 (sessenta) meses.

23.1.3. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração.

23.2.SUPORTE TECNICO LOCAL

23.2.1.1. Durante toda a vigência contratual em conjunto com o suporte técnico oficial do fabricante a CONTRATADA deve prover suporte técnico através de sua própria equipe técnica, o atendimento de primeiro e segundo níveis. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.

23.2.1.2. Em conformidade com a exigência de plantão técnico on-site, a CONTRATADA deve assegurar a disponibilidade de técnicos para deslocamento e atendimento presencial nas dependências das unidades governamentais da Bahia.

23.2.1.3. O atendimento local será acionado sempre que houver perda de conectividade remota com o equipamento ou necessidade de intervenção física (substituição de peças, reconexão de cabos ou restauração de backup via console).

23.2.1.4. Esgotadas as tentativas de solução pela equipe local/remota da revenda, esta terá a obrigação de realizar o escalonamento oficial para a engenharia do fabricante (Vendor Support), mantendo-se responsável pelo acompanhamento do chamado (follow-up) e pela comunicação do status à PRODEB até a resolução definitiva.

23.3.REQUISITOS MINIMOS DE FUNCIONALIDADES

23.3.1. Deverá suportar o acesso via SSH ou WEB (HTTPS) para gerenciamento de soluções. Sendo que o gerenciamento administrativo da solução (configuração de Usuários / relatórios) deve ser realizado através de WEB ou GUI. O acesso SSH deve se dar mais para gerir problemas de hardwares e/ou alterações a nível CLI, para alterações no modo de processamento de pacotes e CPU's e troubleshooting.

23.3.2. Deverá possuir comunicação e autenticação criptografada com usuário e senha na interface gráfica (GUI) e via linha de comando no console de gerenciamento.

23.3.3. Deverá permitir que pelo menos 2 (dois) perfis sejam criados para administração e

monitoramento.

- 23.3.4. Deverá suportar SNMP versão 2 e 3.
- 23.3.5. Deverá permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.
- 23.3.6. Deverá permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.
- 23.3.7. Deverá permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH
- 23.3.8. Deverá possuir autenticação de usuários para acesso à plataforma via LDAP
- 23.3.9. Deverá possuir autenticação de usuários para acesso à plataforma via RADIUS
- 23.3.10. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico.
- 23.3.11. Deverá possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas.
- 23.3.12. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de gráfico.
- 23.3.13. Deverá possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.
- 23.3.14. Deverá possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.
- 23.3.15. Deverá possuir visualização da quantidade de logs enviados de cada dispositivo monitorado.
- 23.3.16. Deverá possuir mecanismos de apagamento automático para logs antigos.
- 23.3.17. Deverá permitir importação e exportação de relatórios.
- 23.3.18. Deverá ter a capacidade de criar relatórios no formato HTML.
- 23.3.19. Deverá ter a capacidade de criar relatórios em formato PDF.
- 23.3.20. Deverá ter a capacidade de criar relatórios no formato XML.
- 23.3.21. Deverá permitir exportar os logs no formato CSV.
- 23.3.22. Deverá gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.
- 23.3.23. Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.

- 23.3.24. Deverá ter relatórios predefinidos.
- 23.3.25. Deverá poder enviar automaticamente os logs para um servidor FTP externo para a solução
- 23.3.26. Deverá permitir a duplicação de relatórios existentes, deve ser possível para edição posterior.
- 23.3.27. Deverá ter a capacidade de personalizar a capa dos relatórios obtidos.
- 23.3.28. Deverá permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.
- 23.3.29. Deverá ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas.
- 23.3.30. Deverá ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real.
- 23.3.31. Deverá permitir que os arquivos de log sejam baixados da plataforma para uso externo.
- 23.3.32. Deverá ter a capacidade de gerar e enviar relatórios periódicos automaticamente.
- 23.3.33. Deverá permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.
- 23.3.34. Deverá permitir o envio por e-mail relatórios automaticamente.
- 23.3.35. Deverá permitir que o relatório seja enviado por e-mail ao destinatário específico.
- 23.3.36. Deverá permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.
- 23.3.37. Deverá exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.
- 23.3.38. Deverá permitir o uso de filtros nos relatórios.
- 23.3.39. Deverá permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.
- 23.3.40. Deverá permitir especificar o idioma dos relatórios criados.
- 23.3.41. Deverá gerar alertas automáticos por e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.
- 23.3.42. Deverá permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.
- 23.3.43. Deverá ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.
- 23.3.44. Deverá possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs

diários recebidos, alertas do sistema, entre outros.

- 23.3.45. Deverá ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.
- 23.3.46. Deverá importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.
- 23.3.47. Deverá ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.
- 23.3.48. Deverá fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.
- 23.3.49. Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.
- 23.3.50. Deverá permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos
- 23.3.51. Deverá permitir visualizar em tempo real os logs recebidos.
- 23.3.52. Deverá permitir o encaminhamento de log no formato syslog.
- 23.3.53. Deverá permitir o encaminhamento de log no formato CEF (Common Event Format).
- 23.3.54. Deverá gerar alertas de eventos a partir de logs recebidos.
- 23.3.55. Deverá permitir a criação de incidentes a partir de alertas de eventos para o terminal.
- 23.3.56. Suportar o padrão SAML ou LDAP ou RADIUS para autenticação do usuário administrador.

23.4.FUNCIONALIDADES DE RELATÓRIOS DE FIREWALL

- 23.4.1. Deverá possuir relatório de conformidade com o PCI DSS.
- 23.4.2. Deverá possuir um relatório de uso do aplicativo SaaS.
- 23.4.3. Deverá possuir um relatório de prevenção de perda de dados (DLP).
- 23.4.4. Deverá possuir um relatório de VPN.
- 23.4.5. Deverá possuir um relatório IPS (Intruder Prevention System).
- 23.4.6. Deverá possuir um relatório de reputação do cliente.
- 23.4.7. Deverá possuir um relatório de análise de segurança do usuário.
- 23.4.8. Deverá possuir um relatório de análise de ameaças cibernéticas.
- 23.4.9. Deverá possuir um breve relatório resumido diário de eventos e incidentes de segurança.
- 23.4.10. Deverá possuir um relatório de tráfego DNS.
- 23.4.11. Deverá possuir um relatório de tráfego de e-mail.
- 23.4.12. Deverá possuir um relatório dos 10 principais aplicativos usados na rede.

23.4.13. Deverá possuir um relatório dos 10 principais sites usados na rede.

23.4.14. Deverá possuir um relatório de uso de mídia social.

23.5.FUNCIONALIDADES DE IOC – INDICADOR DE COMPROMETIMENTO

23.5.1. Deve suportar o serviço de Indicadores de Comprometimento (IoC) de ferramentas do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos:

23.5.1.1. endereço IP do usuário;

23.5.1.2. nome do host;

23.5.1.3. sistema operacional;

23.5.1.4. veredito (classificação geral da ameaça);

23.5.1.5. número de ameaças detectadas

23.6.FUNCIONALIDADE AUTOMAÇÃO PARA DETECÇÃO E RESPOSTA A INCIDENTES

23.6.1. A solução deverá disponibilizar, os recursos de automação. Caso haja necessidade de licenciamento adicional, este deverá estar incluso na proposta.

23.6.2. A solução deverá permitir integração com sistemas de terceiros para utilização em playbooks, contemplando, no mínimo 6 (seis) das seguintes integrações:

23.6.3. FortiGate, JIRA, Microsoft Graph API, Microsoft Management Activity API, Microsoft 365 Defender, Zendesk, FortiClient EMS, AWS Security Hub, Cisco ISE, FortiMail, Nessus, ServiceNow, AWS SQS

23.6.4. A solução deverá possuir capacidade nativa de correlação de logs para identificação de ameaças e eventos de segurança.

23.6.5. A solução deverá dispor de regras de correlação que permitam a agregação de múltiplos eventos para a identificação de ameaças avançadas, com base no modelo Cyber Kill Chain.

23.6.6. As regras de correlação da solução deverão contemplar, no mínimo, os seguintes casos de uso:

23.6.7. Tráfego suspeito em DHCP

23.6.8. Detecção de ataques de phishing

23.6.9. Detecção de ataques DDoS TCP

23.6.10. Alto volume de tráfego DNS

23.6.11. Múltiplas falhas de logon

23.6.12. Comunicação com servidores de Comando e Controle (C&C)

23.6.13. Exfiltração de dados via serviços remotos

23.6.14. Atividade maliciosa em e-mail

- 23.6.15. Detecção de vulnerabilidade Log4J
- 23.6.16. Alteração de membros em grupos
- 23.6.17. A solução deverá permitir a geração de relatórios avançados que correlacionem eventos do SOC, proporcionando visão abrangente (360º) das ameaças detectadas.
- 23.6.18. Os relatórios deverão contemplar, no mínimo, visões alinhadas ao NIST Cybersecurity Framework (CSF), à norma NIST 800-53 e ao padrão IEC 62443.
- 23.6.19. A solução deverá permitir a ingestão de logs oriundos de diversas soluções, por meio de parsers.
- 23.6.20. A solução deverá incluir parsers nativos para, no mínimo 20 (vinte) das seguintes tecnologias:
 - 23.6.20.1. Sophos Firewall, Cisco IOS, Cisco Meraki, Aruba ClearPass, CheckPoint, Fortigate, FortiEMS, SonicWall, Zscaler, McAfee, Palo Alto, Barracuda, CrowdStrike, SentinelOne, Microsoft Defender, ForcePoint, Juniper, Nessus, ServiceNow, Office 365, Okta, Entra ID, AWS Security Hub, AWS CloudTrail, GitLab, Windows, macOS, Linux OS
- 23.6.21. A solução deverá possibilitar a criação de parsers personalizados para integração de soluções não suportadas nativamente.
- 23.6.22. A solução deverá disponibilizar, de forma nativa, playbooks para resposta a incidentes, permitindo a edição dos existentes e a criação de novos fluxos de ação, baseados nas integrações disponíveis.
- 23.6.23. A solução deverá dispor de monitoramento dos Status dos playbooks.
- 23.6.24. Os registros de execução dos playbooks deverão conter, no mínimo: nome, horário de início, horário de término, status final e opção de detalhamento do caso.
- 23.6.25. Para eventos que resultem em incidentes de segurança, a solução deverá possibilitar o registro de um ID único do incidente, categoria, severidade e endpoint(s) afetado(s).
- 23.6.26. Todos os eventos registrados deverão ser exibidos por categoria/severidade, incluindo a possibilidade de exibir mais detalhes do evento.
- 23.6.27. A solução deverá disponibilizar a visualização de todos os ataques ocorridos no ambiente, categorizados conforme a Matriz MITRE ATT&CK, incluindo técnica e tática associadas.

23.7.FUNCIONALIDADES DE IA DO FABRICANTE

- 23.7.1. Deve possuir as funcionalidades de um assistente de segurança de IA generativo integrado à solução para investigação de incidentes, resposta e busca por ameaças.
- 23.7.2. Deve interpretar eventos de segurança, gera resumos, identifica impactos potenciais e

oferece recomendações de remediação.

23.7.3. Deve permitir o uso de prompts de linguagem natural, permitindo criar consultas complexas ao banco de dados, gerar relatórios e executar com eficiência.

23.7.4. Caso a solução a não possua assistente de IA nativo, será permitida a composição com soluções e plataformas de IA generativa complementares desde que devidamente licenciadas, integradas e operacionais e atendendo plenamente aos requisitos técnicos exigidos.

24.LOTE 01 - ITEM 24 - UPGRADE SOLUÇÃO DE DE RELATORIA DE LOGS TIPO 01

24.1.Deve permitir o incremento de 2.000 (dois mil) logs dia da Solução de de Relatoria de Logs Tipo 01.

25.LOTE 01 - ITEM 25 – UST UNIDADE DE SERVIÇOS TECNICOS ESPECIALIZADOS

25.1.Cada Unidade de Serviços Técnicos (UST) corresponderá a atividades relacionadas a serviços de Adequação de Estrutura de Rede Logica, Criação de Ponto de Rede para as Soluções de Conectividade.

25.2.Para realização dos serviços de deve ser utilizadas as quantidades de UST, conforme planilha abaixo:

Tipo Da Atividade	Detalhamento Da Atividade	UST Necessárias
Vistoria Tecnica Tipo 01	Realização de Vistoria Tecnica para verificação de viabilidade técnica de mudança de Endereço da Solução de Conectividade (Firewall e Links de Conectividade) para Capital e localidades até 50 km de Salvador Bahia	01
Vistoria Tecnica Tipo 02	Realização de Vistoria Tecnica para verificação de viabilidade técnica de mudança de Endereço da Solução de Conectividade (Firewall e Links de Conectividade) para localidades de 51 a 300 km de Salvador Bahia	02
Vistoria Tecnica Tipo 03	Realização de Vistoria Tecnica para verificação de viabilidade técnica de mudança de Endereço da Solução de Conectividade (Firewall e Links de Conectividade) para localidades acima de 300 km de Salvador Bahia	03
Organização de Rack Tipo 01	Serviço de higienização, fixação e organização do cabeamento (path cords e elétricos) em rack existente. Inclui fornecimento de insumos de fixação e identificação (abraçadeiras de velcro, etiquetas, porca-gaiola). Não inclui fornecimento de path cords novos ou guias de cabo, salvo se adquiridos em item separado, para Capital e localidades até 50 km de Salvador Bahia. Neste item não esta previsto o fornecimento de cabeamento e itens adicionais, sendo o escopo destas atividades restritas a serviços.	05

Organização de Rack Tipo 02	Serviço de higienização, fixação e organização do cabeamento (path cords e elétricos) em rack existente. Inclui fornecimento de insumos de fixação e identificação (abraçadeiras de velcro, etiquetas, porca-gaiola). Não inclui fornecimento de path cords novos ou guias de cabo, salvo se adquiridos em item separado, para localidades de 51 a 300 km de Salvador Bahia. Neste item não está previsto o fornecimento de cabeamento e itens adicionais, sendo o escopo destas atividades restritas a serviços.	06
Organização de Rack Tipo 03	Serviço de higienização, fixação e organização do cabeamento (path cords e elétricos) em rack existente. Inclui fornecimento de insumos de fixação e identificação (abraçadeiras de velcro, etiquetas, porca-gaiola). Não inclui fornecimento de path cords novos ou guias de cabo, salvo se adquiridos em item separado, para localidades acima 300 km de Salvador Bahia. Neste item não está previsto o fornecimento de cabeamento e itens adicionais, sendo o escopo destas atividades restritas a serviços.	07
Confecção de Ponto de Rede Tipo 01	Fornecimento e instalação de até 05 pontos de rede lógica. Inclui: lançamento de cabo UTP Categoria 5E (CAT5E) homologado Anatel (até 75m), conectorização em ambas as pontas (Keystone/RJ45 Macho), identificação (etiquetagem), testes de continuidade e fornecimento de infraestrutura aparente (canaleta de PVC ou similar) até 3 metros por ponto, para Capital e localidades até 50 km de Salvador Bahia.	10
Confecção de Ponto de Rede Tipo 02	Fornecimento e instalação de até 05 pontos de rede lógica. Inclui: lançamento de cabo UTP Categoria 5E (CAT5E) homologado Anatel (até 75m), conectorização em ambas as pontas (Keystone/RJ45 Macho), identificação (etiquetagem), testes de continuidade e fornecimento de infraestrutura aparente (canaleta de PVC ou similar) até 3 metros por ponto, para localidades de 51 a 300 km de Salvador	11
Confecção de Ponto de Rede Tipo 03	Fornecimento e instalação de até 05 pontos de rede lógica. Inclui: lançamento de cabo UTP Categoria 5E (CAT5E) homologado Anatel (até 75m), conectorização em ambas as pontas (Keystone/RJ45 Macho), identificação (etiquetagem), testes de continuidade e fornecimento de infraestrutura aparente (canaleta de PVC ou similar) até 3 metros por ponto, para localidades acima de 300 km de Salvador	12
Confecção de Ponto de Rede Tipo 04	Fornecimento e instalação de até 10 pontos de rede lógica. Inclui: lançamento de cabo UTP Categoria 5E (CAT5E) homologado Anatel (até 75m), conectorização em ambas as pontas (Keystone/RJ45 Macho), identificação (etiquetagem), testes de continuidade e fornecimento de infraestrutura aparente (canaleta de PVC ou similar) até 3 metros por ponto, para Capital e localidades até 50 km de Salvador Bahia.	16
Confecção de Ponto de Rede Tipo 05	Fornecimento e instalação de até 10 pontos de rede lógica. Inclui: lançamento de cabo UTP Categoria 5E	17

	(CAT5E) homologado Anatel (até 75m), conectorização em ambas as pontas (Keystone/RJ45 Macho), identificação (etiquetagem), testes de continuidade e fornecimento de infraestrutura aparente (canaleta de PVC ou similar) até 3 metros por ponto, para localidades de 51 a 300 km de Salvador	
Confecção de Ponto de Rede Tipo 06	Fornecimento e instalação de até 10 pontos de rede lógica. Inclui: lançamento de cabo UTP Categoria 5E (CAT5E) homologado Anatel (até 75m), conectorização em ambas as pontas (Keystone/RJ45 Macho), identificação (etiquetagem), testes de continuidade e fornecimento de infraestrutura aparente (canaleta de PVC ou similar) até 3 metros por ponto, para localidades acima de 300 km de Salvador	18

25.3.DINÂMICA DE CONTRATAÇÃO:

- 25.3.1. A LICITANTE contratará a quantidade de Unidades de Serviços Técnicos estimadas para consumo pelo período desejado durante a vigência do contrato. Emitirá nota(s) de empenho para adquirir vouchers para quantidade de Unidades de Serviços Técnicos estimados para o período correspondente.
- 25.3.2. A CONTRATADA deve entregar os vouchers relativos à quantidade de Unidades de Serviços contratadas que poderão ser consumidos pela LICITANTE ao longo do período do contrato de acordo com a sua necessidade;
- 25.3.3. A CONTRATANTE consultará a CONTRATADA para calcular a quantidade de Unidades de Serviços Técnicos necessárias para realizar a atividade pretendida e emitirá Ordem de Serviço para a CONTRATADA prestar os serviços. E, ao final dos serviços, contabilizará o consumo das Unidades de Serviços Técnico utilizadas;
- 25.3.4. O prazo máximo para início das atividades pela empresa contratada será de 20 (vinte) dias;
- 25.3.5. As UST executadas fora do expediente comercial por solicitação da CONTRATANTE, serão contabilizadas em dobro;
- 25.3.6. A empresa CONTRATADA deve nomear funcionário capacitado que será responsável por fornecer aconselhamento técnico e operacional sobre os serviços; assistência sobre as condições do contrato; gerenciamento de escalação junto ao Fabricante; Gerenciamento de recursos e cronograma de entrega dos serviços;
- 25.3.7. Neste modelo de execução dos serviços não se caracteriza a subordinação direta e nem a pessoalidade, visto que não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da empresa contratada e este Órgão. As empresas proponentes

deverão considerar em seus custos todos os recursos necessários ao completo atendimento aos objetos, tais como despesas com pessoal (salários, férias, encargos, benefícios, seleção, outras) de modo a garantir os serviços definidos;

- 25.3.8. Para o controle da execução dos serviços será utilizado a Unidade de medida UST (Unidade de Serviço Técnico). A UST consiste na "moeda" usada para dimensionar todas as atividades que serão demandadas pela CONTRATANTE, no escopo de cada Ordem de Serviço. A contratação será em volume de UST por atividade e a licitação resultará na oferta do valor de uma UST que irá representar o esforço combinado de profissionais envolvidos, variando a complexidade e prioridade da atividade.

25.4. ETAPAS:

25.4.1. Iniciação:

- 25.4.1.1. Avaliação do cenário da CONTRATANTE: Realização de uma análise completa do ambiente do cliente para entender suas necessidades específicas.
- 25.4.1.2. Desenvolvimento de plano de implementação: Criação de um plano detalhado que delinea as etapas e os recursos necessários para a implementação bem-sucedida do projeto.

25.4.2. Planejamento:

- 25.4.2.1. Elaboração de uma estratégia abrangente que inclui o cronograma de implementação, controle de prazos, esforço, vistoria (quando houver serviço de Criação de Infraestrutura contratado), atribuição de responsabilidades, alocação de recursos, indicadores do projeto e qualquer outra métrica prevista no PMBOK. O objetivo de todas estas atividades é a garantia de qualidade do projeto no que tange prazos e esforço.

25.4.3. Execução:

- 25.4.3.1. Análise: Realização de uma análise minuciosa dos requisitos e processos da CONTRATANTE para garantir que a solução proposta seja adequada.
- 25.4.3.2. Configuração: Personalização da solução de acordo com as necessidades específicas da CONTRATANTE ajustando as configurações e os parâmetros de rede.
- 25.4.3.3. Infraestrutura: Fixação dos equipamentos em racks; realizações das conexões de patch-cords.
- 25.4.3.4. Integração: Integração da solução com os sistemas existentes, garantindo a interoperabilidade e o fluxo de dados adequado.
- 25.4.3.5. Testes, otimização e ajustes: Realização de testes para verificar a funcionalidade e estabilidade da solução implantada. A partir dos resultados, implementamos melhorias

e ajustes para otimizar o desempenho e garantir o resultado esperado.

25.4.4. Encerramento:

25.4.4.1. Documentação: Elaboração de documentação que descreve a solução implantada conforme construída.

LOTE 02

26.LOTE - 02 - ITEM 01 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 600E

26.1.CARACTERÍSTICAS GERAIS:

26.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-600E, SKU FC-10-F6H0E-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN.

27.LOTE - 02 - ITEM 02 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 601E

27.1.CARACTERÍSTICAS GERAIS:

27.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-601E, SKU FC-10-F6H1E-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN.

28.LOTE - 02 - ITEM 03 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 400F

28.1.CARACTERÍSTICAS GERAIS:

28.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-400F, SKU FC-10-0400F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN.

29.LOTE - 02 - ITEM 04 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 200F

29.1.CARACTERISTICAS GERAIS:

- 29.1.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-200F, SKU FC-10-200F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN.

30.LOTE - 02 - ITEM 05 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 200E

30.1.CARACTERISTICAS GERAIS:

- 30.1.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-200E, SKU FC-10-00207-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN.

31.LOTE - 02 - ITEM 06 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 100F

31.1.CARACTERISTICAS GERAIS:

- 31.1.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-100F, SKU FC-10-F100F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN.

32.LOTE - 02 - ITEM 07 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 80F

32.1.CARACTERISTICAS GERAIS:

- 32.1.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-80F, SKU FC-10-0080F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações,

Otimização WAN.

33.LOTE - 02 - ITEM 08 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 60F

33.1.CARACTERISTICAS GERAIS:

- 33.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-60F, SKU FC-10-0060F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN.

34.LOTE - 02 - ITEM 09 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 61F

34.1.CARACTERISTICAS GERAIS:

- 34.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-61F, SKU FC-10-0061F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN.

35.LOTE - 02 - ITEM 10 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DE RESPOSITORIO E RELATORIA DE LOGS MARCA FORTINET E MODELO FORTIANALYZER 150G

35.1.CARACTERISTICAS GERAIS:

- 35.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FAZ-150G, SKU FC-10-L150G-247-02-12, pelo período de 12 (doze) meses.

36.LOTE - 02 - ITEM 11 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DE RESPOSITORIO E RELATORIA DE LOGS MARCA FORTINET E MODELO FORTIANALYZER 300G

36.1.CARACTERISTICAS GERAIS:

- 36.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FAC-300G, SKU FC-10-L03HG-247-02-12, pelo período de 12

(doze) meses.

37.LOTE - 02 - ITEM 12 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES AUTENTICAÇÃO DE USUARIO MARCA FORTINET MODELO FORTIAUTHENTICATOR 800F

37.1.CARACTERISTICAS GERAIS:

- 37.1.1. Licenciamento e Serviços de Garantia Técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FAC-800F, SKU FC-10-AC8HF-247-02-12, pelo período de 12 (doze) meses.

38.LOTE - 02 - ITEM 13 - SOLUÇÃO DE SEGURANÇA DE REDE NGFW – TIPO I

- 38.1.A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.
- 38.2.Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance físico), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;
- 38.3.A solução poderá ser composta por mais de um equipamento para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 38.4.A solução deve permitir acesso a gerência e monitoramento, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
- 38.5.A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.
- 38.6.Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
- 38.7.Deve possuir e estar licenciado durante a vigência contratual de 12 (doze) meses, minimamente

com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.

- 38.8. Deve suportar no mínimo 25 (vinte e cinco) instâncias virtuais de firewall e estar licenciado para no mínimo 10 (dez) instâncias virtuais de firewall;
- 38.9. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 38.10. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 38.11. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 38.12. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 38.13. Deve possuir firewall com capacidade mínima de processamento de 150 (cento e cinquenta) Gbps.
 - 38.13.1. Deve possuir IPS com capacidade mínima de processamento de 40 (quarenta) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 38.14. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 30 (trinta) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 38.15. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 15 (quinze) Gbps.
- 38.16. Deve possuir VPN com capacidade de, pelo menos, 50 (cinquenta) Gbps de tráfego IPSec.
- 38.17. Deve suportar 15.000.000 (quinze milhões) conexões simultâneas.

- 38.18. Deve suportar, pelo menos, 700.000 (setecentas mil) novas conexões por segundo.
- 38.19. Deve suportar, pelo menos, 2000 (dois mil) túneis de VPN Site-Site.
- 38.20. Deve suportar, pelo menos, 45.000 (quarenta e cinco mil) túneis de VPN Client-Site.
- 38.21. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE.
- 38.22. Deve possuir, pelo menos, 4 (quatro) interfaces SFP28 25GE.
- 38.23. Deve possuir, pelo menos, 4 (quatro) interfaces SFP+ 10GE.
- 38.24. Deve possuir, pelo menos, 1 (uma) interface RJ45 2.5GE.
- 38.25. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 38.26. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 38.27. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.
- 38.28. SERVIÇOS DE GARANTIA TÉCNICA LOCAL
- 38.28.1.1. Durante toda a vigência contratual em conjunto com os serviços de garantia técnica oficial do fabricante a CONTRATADA deve prover os serviços através de sua própria equipe técnica, o atendimento de primeiro e segundo níveis. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.
- 38.28.1.2. Em conformidade com a exigência de plantão técnico on-site, a CONTRATADA deve assegurar a disponibilidade de técnicos para deslocamento e atendimento presencial nas dependências das unidades governamentais da Bahia.
- 38.28.1.3. O atendimento local será acionado sempre que houver perda de conectividade remota com o equipamento ou necessidade de intervenção física (substituição de peças, reconexão de cabos ou restauração de backup via console).
- 38.28.1.4. Esgotadas as tentativas de solução pela equipe local/remota da revenda, esta terá a obrigação de realizar o escalonamento oficial para a engenharia do fabricante (Vendor Support), mantendo-se responsável pelo acompanhamento do chamado (follow-up) e pela comunicação do status à PRODEB até a resolução definitiva
- 38.29. FUNCIONALIDADES DE FIREWALL
- 38.29.1.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.

- 38.29.1.2. Possuir suporte a sub-interfaces ethernet lógicas;
- 38.29.1.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.
- 38.29.1.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.
- 38.29.1.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 38.29.1.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 38.29.1.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 38.29.1.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 38.29.1.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 38.29.1.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 38.29.1.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 38.29.1.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 38.29.1.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 38.29.1.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 38.29.1.15. Deve suportar o encaminhamento de tráfego multicast.
- 38.29.1.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 38.29.1.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 38.29.1.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 38.29.1.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 38.29.1.20. Suportar OSPF gracefulrestart;
- 38.29.1.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

- 38.29.1.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 38.29.1.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 38.29.1.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 38.29.1.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 38.29.1.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 38.29.1.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 38.29.1.28. Drop sem notificação do bloqueio ao usuário;
 - 38.29.1.29. Drop com notificação do bloqueio ao usuário;
 - 38.29.1.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 38.29.1.31. TCP-Reset para o cliente;
 - 38.29.1.32. TCP-Reset para o server ou para os dois lados da conexão.
- 38.29.1.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 38.29.1.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 38.29.1.35. Deve oferecer suporte ao protocolo SIP.
- 38.29.1.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 38.29.1.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 38.29.1.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 38.29.1.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações

que utilizem portas variáveis.

- 38.29.1.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 38.29.1.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 38.29.1.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 38.29.1.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 38.29.1.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 38.29.1.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 38.29.1.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 38.29.1.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 38.29.1.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 38.29.1.49. Realizar Traffic Shaping para a solução de segurança
- 38.29.1.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 38.29.1.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 38.29.1.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 38.29.1.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 38.29.1.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 38.29.1.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA)

utilizando tokens.

- 38.29.1.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 38.29.1.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 38.29.1.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 38.29.1.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 38.29.1.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 38.29.1.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 38.29.1.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 38.29.1.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 38.29.1.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 38.29.1.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 38.29.1.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 38.29.1.67. Funcionar com tradução de porta (PAT);
- 38.29.1.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 38.29.1.69. Implementar e suportar NAT64 e NAT46;
- 38.29.1.70. Implementar NAT66
- 38.29.1.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 38.29.1.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 38.29.1.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 38.29.1.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os

protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.

38.29.1.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:

38.29.1.75.1. Conectores SDN Privados:

- 38.29.1.75.1.1. Nutanix;
- 38.29.1.75.1.2. Kubernetes;
- 38.29.1.75.1.3. VMware ESXi;
- 38.29.1.75.1.4. OpenStack;

38.29.1.75.2. Conectores SDN Públicos;

- 38.29.1.75.2.1. Google Cloud Platform (GCP);
- 38.29.1.75.2.2. AWS;
- 38.29.1.75.2.3. Microsoft Azure;
- 38.29.1.75.2.4. Oracle Cloud Infrastructure (OCI);

38.29.1.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).

38.29.1.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;

38.29.1.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).

38.29.1.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.

38.29.1.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

38.29.2. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

38.29.2.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.

- 38.29.2.2. Deve permitir modificação de valores DSCP para o DiffServ.
- 38.29.2.3. Deve permitir priorização de tráfego e suportar ToS.
- 38.29.2.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
- 38.29.2.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 38.29.2.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 38.29.2.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 38.29.2.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 38.29.2.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
- 38.29.2.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

38.29.3. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

- 38.29.3.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
- 38.29.3.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
- 38.29.3.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
- 38.29.3.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 38.29.3.5. Deve permitir a criação de categorias personalizadas.
- 38.29.3.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 38.29.3.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 38.29.3.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 38.29.3.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 38.29.3.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação

de URL;

- 38.29.3.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 38.29.3.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 38.29.3.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 38.29.3.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 38.29.3.15. Permitir a criação de categorias de URLs customizadas;
- 38.29.3.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 38.29.3.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 38.29.3.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 38.29.3.19. Permitir a customização de página de bloqueio;
- 38.29.3.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 38.29.3.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 38.29.3.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 38.29.3.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 38.29.3.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 38.29.3.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo

endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

- 38.29.3.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
 - 38.29.3.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
 - 38.29.3.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
 - 38.29.3.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
 - 38.29.3.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
 - 38.29.3.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
 - 38.29.3.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
 - 38.29.3.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
 - 38.29.3.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
 - 38.29.3.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
 - 38.29.3.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
 - 38.29.3.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
 - 38.29.3.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
 - 38.29.3.39. Deve possuir Proxy Explícito e Transparente.
 - 38.29.3.40. Deve implementar roteamento WCCP e ICAP.
- 38.29.4. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)
- 38.29.4.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
 - 38.29.4.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.

- 38.29.4.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 38.29.4.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 38.29.4.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 38.29.4.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 38.29.4.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 38.29.4.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 38.29.4.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 38.29.4.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 38.29.4.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 38.29.4.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 38.29.4.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 38.29.4.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 38.29.4.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 38.29.4.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 38.29.4.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 38.29.4.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer

Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).

- 38.29.4.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 38.29.4.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 38.29.4.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 38.29.4.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 38.29.4.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 38.29.4.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 38.29.4.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 38.29.4.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 38.29.4.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 38.29.4.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 38.29.4.29. Identificar, alertar e bloquear comunicação com botnets;
- 38.29.4.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 38.29.4.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 38.29.4.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 38.29.4.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido

o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

- 38.29.4.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
 - 38.29.4.35. Identificar nos eventos o país de onde partiu a ameaça;
 - 38.29.4.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
 - 38.29.4.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
 - 38.29.4.38. Deve possuir alarmes na console de administração.
 - 38.29.4.39. Deve possuir alertas via correio eletrônico.
 - 38.29.4.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
 - 38.29.4.41. Deve ter a capacidade de resposta/logs ativa a ataques.
 - 38.29.4.42. Incluir proteção contra ataques de negação de serviços (DoS);
 - 38.29.4.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
 - 38.29.4.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;
- 38.29.5. FUNCIONALIDADE DE VPN
- 38.29.5.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
 - 38.29.5.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
 - 38.29.5.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
 - 38.29.5.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
 - 38.29.5.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
 - 38.29.5.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
 - 38.29.5.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;

- 38.29.5.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
- 38.29.5.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 38.29.5.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 38.29.5.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 38.29.5.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 38.29.5.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 38.29.5.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 38.29.5.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 38.29.5.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 38.29.5.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPSec estabelecidos.
- 38.29.6. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
 - 38.29.6.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
 - 38.29.6.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
 - 38.29.6.3. Atualizar a base de assinaturas de aplicações automaticamente;
 - 38.29.6.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
 - 38.29.6.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de

aplicações em algumas regras;

- 38.29.6.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 38.29.6.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 38.29.6.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 38.29.6.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 38.29.6.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 38.29.6.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 38.29.6.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 38.29.6.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 38.29.6.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 38.29.6.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 38.29.6.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 38.29.6.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 38.29.6.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.

- 38.29.6.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 38.29.6.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 38.29.6.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 38.29.6.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 38.29.6.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 38.29.6.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 38.29.6.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 38.29.6.26. Deve permitir criação de padrões de aplicação manualmente.
- 38.29.6.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 38.29.6.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 38.29.6.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 38.29.6.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;
- 38.29.7. FUNCIONALIDADE DE SD-WAN
 - 38.29.7.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
 - 38.29.7.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.
 - 38.29.7.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;

- 38.29.7.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
- 38.29.7.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
- 38.29.7.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 38.29.7.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 38.29.7.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;
- 38.29.7.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 38.29.7.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 38.29.7.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 38.29.7.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 38.29.7.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 38.29.7.14. Passivo: uso do tráfego real para as medições;
- 38.29.7.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 38.29.7.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 38.29.7.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.

- 38.29.7.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 38.29.7.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 38.29.7.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 38.29.7.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 38.29.7.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 38.29.7.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 38.29.7.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 38.29.7.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 38.29.7.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 38.29.7.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 38.29.7.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva,

objetivando uma melhor experiência de uso de aplicações de negócio;

- 38.29.7.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;

38.30. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

- 38.30.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:
- 38.30.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.
- 38.30.1.2. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.
- 38.30.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:
- 38.30.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.
- 38.30.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.
- 38.30.2.3. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

39.LOTE - 02 - ITEM 14 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE SEGURANÇA DE REDE NGFW – TIPO I

CARACTERÍSTICAS GERAIS:

- 39.1.1. Licenciamento e Garantia Técnica do Fabricante para o ITEM SOLUÇÃO DE SEGURANÇA DE REDE NGFW – TIPO I, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.
- 39.1.2. Durante toda a vigência contratual em conjunto com os serviços de garantia técnica oficial do fabricante a CONTRATADA deve prover serviços on-site através de sua própria equipe técnica. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.

40.LOTE - 02 - ITEM 15 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 3700F

40.1.CARACTERISTICAS GERAIS:

- 40.1.1.1. Licenciamento e serviços de garantia técnico do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-3700F, SKU FC-10-F3K7F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.

41.LOTE - 02 - ITEM 16 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 3301E

41.1.CARACTERISTICAS GERAIS:

- 41.1.1.1. Licenciamento e serviços de garantia técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-3301E, SKU FC-10-F33E1-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.

42.LOTE - 02 - ITEM 17 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 3000D

42.1.CARACTERISTICAS GERAIS:

- 42.1.1.1. Licenciamento e serviços de garantia técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-3000D, SKU FC-10-03007-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.

43.LOTE - 02 - ITEM 18 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 600F

43.1.CARACTERISTICAS GERAIS:

- 43.1.1.1. Licenciamento e serviços de garantia técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-600F, SKU FC-10-0600F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações,

Otimização WAN.

44.LOTE - 02 - ITEM 19 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE 40F

44.1.CARACTERÍSTICAS GERAIS:

- 44.1.1. Licenciamento e serviços de garantia técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-40F, SKU FC-10-0040F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN.

45.LOTE - 02 - ITEM 20 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES NGFW MARCA FORTINET MODELO FORTIGATE VM08

45.1.CARACTERÍSTICAS GERAIS:

- 45.1.1. Licenciamento e serviços de garantia técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FG-VM08, SKU FC-10-FVM08-963-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN

46.LOTE - 02 - ITEM 21 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DE WAF MARCA FORTINET MODELO FORTIWEB 2000F

46.1.CARACTERÍSTICAS GERAIS:

- 46.1.1. Licenciamento e serviços de garantia técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FortiWeb, SKU FC-10-FW2KF-580-02-12, pelo período de 12 (doze) meses das funcionalidades: Advanced Bundle - Standard Bundle plus Credential Stuffing Defense Service and Threat Analytics.

47.LOTE - 02 - ITEM 22 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES ADC MARCA FORTINET E MODELO FORTIADC 400F

47.1.CARACTERÍSTICAS GERAIS:

- 47.1.1. Licenciamento e serviços de garantia técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FortiADC 400F, SKU FC-10-AD4HF-731-02-12, pelo período de 12 (doze) meses das funcionalidades: Application Security - Network Security Bundle Plus WAF

Signatures, WAF Adaptive Learning, FortiADC Cloud Sandbox, Credential Stuffing Defense, FortiGuard Data Loss Prevention Service, and FortiCare Premium.

48.LOTE - 02 - ITEM 23 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES GERENCIADOR CENTRALIZADA DE DISPOSITIVOS, MARCA FORTINET MODELO FORTIMANAGER 3000G

48.1.CARACTERÍSTICAS GERAIS:

- 48.1.1. Licenciamento e serviços de garantia técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FMG-3000G, SKU FC-10-M03KG-247-02-12, pelo período de 12 (doze) meses.

49.LOTE - 02 - ITEM 24 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES SOLUÇÃO DE SIEM MARCA FORTINET MODELO FORTISIEM VM

49.1.CARACTERÍSTICAS GERAIS:

- 49.1.1. Licenciamento e serviços de garantia técnica do Fabricante para os equipamentos do Fabricante Fortinet Modelo FortiSiem VM - 4000 Points, SKU FCC-10-FSM97-248-02-12, pelo período de 12 (doze) meses.

50.LOTE - 02 - ITEM 25 – Serviço de Upgrade para 50 Devices e 500 EPS de SIEM MARCA FORTINET MODELO FORTISIEM VM

50.1.CARACTERÍSTICAS GERAIS:

- 50.1.1. Licenciamento para upgrade de 50 Devices e 500 EPS para os equipamentos do Fabricante Fortinet Modelo FortiSiem VM - 4000 Points, SKU: FSM-AIO-50-UG

51.LOTE - 02 - ITEM 26 – SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAF – TIPO 01

51.1.CARACTERÍSTICAS E FUNCIONALIDADES GERAIS

- 51.1.1. A solução deverá ser fornecida na forma de appliance físico, por motivos de segurança, não serão aceitos equipamentos de propósito genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de uso geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.
- 51.1.2. A solução poderá ser composta por mais de um equipamento para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração. A ocupação total no rack não deverá exceder 4U.

- 51.1.3. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados para funcionar dessa forma.
- 51.1.4. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze) meses, minimamente com as seguintes funcionalidades: Antivírus, Reputação de IP, Sandbox, Serviço de Defesa de Preenchimento de Credenciais e Análise Avançada de Ameaças.
- 51.1.5. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Monitoramento e Relatoria de Logs existente na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F. Caso o item não atenda a esta exigência será preciso entregar solução equivalente de capacidade igual ou superior.
- 51.1.6. REQUISITOS MÍNIMOS DE PERFORMANCE
- 51.1.7. Deve possuir throughput para proteção de aplicações Web de mínimo de 5 (cinco) Gbps.
- 51.1.8. Deve possuir, pelo menos, 04 (quatro) interfaces SFP 1GE.
- 51.1.9. Deve possuir, pelo menos, 04 (quatro) interfaces RJ45 1GE.
- 51.1.10. Deve possuir, pelo menos, 400 GB SSD de armazenamento interno.
- 51.1.11. Deve possuir, pelo menos, 02 (duas) interfaces SFP+ 10GE
- 51.1.12. Deve suportar quantidade ilimitada de aplicações protegidas.
- 51.1.13. FUNCIONALIDADES DE REDE
- 51.1.14. A solução deve ser capaz de ser implementada nos modos de operação Proxy Reverso, Proxy Transparente (Inline), Modo Passivo ou Sniffer (Offline), e Bridge Transparente. Deve ainda ser capaz de ser implementada com o protocolo WCCP.
- 51.1.15. Suportar VLANs no padrão IEEE 802.1Q.
- 51.1.16. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP) - IEEE 802.3ad.
- 51.1.17. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs).
- 51.1.18. A solução deve suportar roteamento por política (policy route).
- 51.2.FUNCIONALIDADES DE GERÊNCIA
- 51.2.1. A solução deve oferecer interface gráfica web (GUI) para configuração e monitoramento, acessível via navegadores gratuitos utilizando o protocolo HTTPS. Também deve permitir administração via CLI, tanto localmente (porta de console) quanto remotamente via SSH.
- 51.2.2. A interface gráfica deve apresentar informações completas sobre o sistema, incluindo cluster, hostname, número de série, modo de operação, uptime, versão do firmware,

licenciamento, consumo de CPU, memória, estatísticas de conexões, throughput HTTP, requisições, eventos e logs recentes.

- 51.2.3. A administração da solução deve permitir o uso de perfis de acesso.
- 51.2.4. A solução deve permitir backup e restauração pela interface gráfica, com suporte a criptografia e utilização dos protocolos FTP, SFTP, TFTP ou HTTPS.
- 51.2.5. Deve ser possível instalar uma versão alternativa do firmware no disco e inicializá-la manualmente em caso de falha do firmware principal.
- 51.2.6. Deve suportar SNMP (v1, v2c e v3), envio de eventos via e-mail, traps SNMP e Syslog, e armazenar logs localmente e remotamente.
- 51.2.7. A solução deve permitir a adição de identificadores personalizados nos registros Syslog, como o hostname, podendo ser fixos ou variáveis.
- 51.2.8. Deve permitir o envio de alertas por e-mail baseados na severidade e/ou categoria dos eventos.
- 51.2.9. O dashboard deve exibir os últimos logs de ataques detectados ou bloqueados.
- 51.2.10. A interface gráfica deve mostrar o consumo de memória em tempo real.
- 51.2.11. A utilização de disco para armazenamento de logs deve ser acessível via interface gráfica ou CLI.
- 51.2.12. Devem estar disponíveis estatísticas de conexões simultâneas e por segundo, com base nas políticas de segurança.
- 51.2.13. A solução deve exibir estatísticas em tempo real de throughput HTTP, eventos de ataques, requisições HTTP e os últimos eventos do sistema.
- 51.2.14. A interface gráfica deve incluir um painel com informações sobre as interfaces de rede.
- 51.2.15. As informações de licenciamento e assinaturas devem estar disponíveis na interface gráfica.
- 51.2.16. A solução deve oferecer análise geográfica dos acessos web.
- 51.2.17. A solução deve apresentar dados analíticos com total e percentual de ataques, tráfego e acessos (hits), por país de origem.
- 51.2.18. Deve ser possível gerar relatórios detalhados com base em tráfego, acessos e atividades de usuários.
- 51.2.19. A solução deve oferecer suporte a APIs RESTful para gerenciamento de configurações.
- 51.2.20. Deve suportar comunicação com protocolo HTTP/2.
- 51.2.21. FUNCIONALIDADES DE AUTENTICAÇÃO
- 51.2.22. A solução deve permitir autenticação de usuários por meio do cabeçalho HTTP/HTTPS

Authorization.

- 51.2.23. Deve suportar autenticação via formulários HTML embutidos em páginas web.
- 51.2.24. Deve permitir a autenticação de usuários com uso de certificados digitais pessoais.
- 51.2.25. A solução deve dispor de uma base local para cadastro e autenticação de contas de usuários.
- 51.2.26. Deve ser compatível com autenticação de usuários em diretórios externos, como LDAP e RADIUS.
- 51.2.27. Deve permitir autenticação via NTLM, utilizando contas de usuários armazenadas em servidores remotos.
- 51.2.28. A solução deve possibilitar a criação de grupos de usuários para aplicação de políticas de acesso comuns durante o processo de autenticação.

51.3.FUNCIONALIDADES DE WEB APPLICATION FIREWALL

- 51.3.1. Deve ser capaz de identificar e bloquear ataques através de um banco de dados de assinaturas de vírus e IP reputation, atualizado de forma automática.
- 51.3.2. Deve implementar recursos de Sandbox para análise de malware moderno;
- 51.3.3. Deve implementar recurso de machine learning, onde será permitido implementar proteção para um servidor ou grupo de servidores de aplicação web, de forma automatizada através da análise da utilização da aplicação, fazendo a descoberta da estrutura e padrões e padrões de uso, buscando separar o comportamento anormal do abusivo, detectando anomalias e tentativas de ataque.
- 51.3.4. Deve implementar proteção contra a lista de técnicas/ataques listados no OWASP 10 (Open Web Application security Project)
- 51.3.5. Deve implementar recursos embarcados de antivírus para análise de arquivos, detecção e bloqueio de malwares que possam comprometer os servidores possuindo integração com a nuvem do fabricante para obter atualizações, enviar e receber amostras de malware para análise/verificação.
- 51.3.6. Ter a capacidade de criação de assinaturas de ataque customizáveis.
- 51.3.7. Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol.
- 51.3.8. Ter a capacidade de proteção para ataques do tipo Botnet.
- 51.3.9. Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST).
- 51.3.10. A solução Deve possuir funcionalidade de proteção positiva contra-ataques como acesso por força bruta.

- 51.3.11. Deve suportar detecção a ataques de Clickjacking.
- 51.3.12. Deve suportar detecção a ataques de alteração de cookie.
- 51.3.13. Deve identificar e prevenir ataques do tipo Credit Card Theft.
- 51.3.14. Deve identificar e prevenir ataques Cross Site Request Forgery (CSRF).
- 51.3.15. A solução deve possuir funcionalidade de proteção positiva contra-ataques como cross site scripting (XSS).
- 51.3.16. Deve possuir proteção contra ataques de Denial of Service (DoS).
- 51.3.17. Deve possuir a capacidade de proteção para ataques do tipo HTTP header overflow.
- 51.3.18. Deve possuir a capacidade de proteção para ataques do tipo Local File inclusion (FLI).
- 51.3.19. Deve possuir a capacidade de proteção para ataques do tipo Man-in-the-middle (MITM).
- 51.3.20. Deve possuir a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI).
- 51.3.21. Deve possuir a capacidade de proteção para ataques do tipo Server Information Leakage.
- 51.3.22. Deve possuir proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection).
- 51.3.23. Deve possuir a capacidade de proteção para ataques do tipo Malformed XML.
- 51.3.24. Deve Identificar e prevenir ataques do tipo Low-rate DoS.
- 51.3.25. Deve possuir prevenção contra Slow POST attack.
- 51.3.26. Deve proteger contra-ataques Slowloris.
- 51.3.27. Deve possuir a capacidade de proteção para ataques do tipo SYN flood.
- 51.3.28. Deve possuir a capacidade de proteção para ataques do tipo Forms Tampering.
- 51.3.29. A solução deve possuir funcionalidade de proteção positiva contra-ataques de manipulação de campo escondido.
- 51.3.30. Deve possuir a capacidade de proteção para ataques do tipo Directory Traversal.
- 51.3.31. Deve possuir a capacidade de proteção do tipo Access Rate Control.
- 51.3.32. Deve possuir a habilidade de configurar proteção do tipo TCP SYN flood-style para prevenção de DoS para qualquer política, através de Syn Cookie e Half Open Threshold.
- 51.3.33. Deve permitir configurar regras de bloqueio a métodos HTTP indesejados.
- 51.3.34. Deve permitir que sejam configuradas regras de limite de upload por tamanho de arquivo.
- 51.3.35. Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país.

- 51.3.36. Deve permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem.
- 51.3.37. Deve permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.
- 51.3.38. Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation.
- 51.3.39. Deve possuir a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP.
- 51.3.40. Deve possuir a funcionalidade de proteger o website contra ações de desfiguração (defacement), com restauração automática e rápida do site caso ocorra à falha.
- 51.3.41. Deve possuir a funcionalidade de antivírus para inspeção de tráfego e arquivos.
- 51.3.42. Deve ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia.
- 51.3.43. A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego.
- 51.3.44. Deve para SSL/TLS offload suportar no mínimo TLS 1.0, 1.1, 1.2 e 1.3.
- 51.3.45. A solução deve ter a capacidade de armazenar certificados digitais de CA's.
- 51.3.46. A solução deve ser capaz de gerar CSR para ser assinado por uma CA.
- 51.3.47. A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL).
- 51.3.48. A solução deve conter as assinaturas de robôs conhecidos como link checkers, indexadores de web, search engines, spiders e web crawlers que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões.
- 51.3.49. A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers etc. Tal sistema deve ser atualizado automaticamente.
- 51.3.50. A solução Deve ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores.
- 51.3.51. A solução deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location.
- 51.3.52. A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessadas para prevenir ataques como cross-site request forgery (CSRF).
- 51.3.53. A solução deve ter a capacidade de definir restrições a métodos HTTP.

- 51.3.54. A solução deve ter a capacidade de proteger contra a detecção de campos ocultos.
- 51.3.55. Deve permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares.
- 51.3.56. A solução deve incluir capacidade de atuar como um scanner de vulnerabilidades ou permitir a integração com scanners de vulnerabilidade de terceiros para diagnóstico e identificação de ameaças nos servidores web, software desatualizado e potenciais buffers overflows,
 - 51.3.56.1. Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros.
 - 51.3.56.2. A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML.
 - 51.3.56.3. A solução deve permitir a exclusão de URLs na análise de vulnerabilidades.
 - 51.3.56.4. Deve ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente.
 - 51.3.56.5. Deve suportar redireção e reescrita de requisições e respostas HTTP.
 - 51.3.56.6. Deve permitir redirecionar requisições HTTP para HTTPS.
 - 51.3.56.7. Deve permitir reescrever a linha URL no cabeçalho de uma requisição HTTP.
 - 51.3.56.8. Deve permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP.
 - 51.3.56.9. Deve permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP.
 - 51.3.56.10. Deve permitir redirecionar requisições para outro web site.
 - 51.3.56.11. Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP.
 - 51.3.56.12. Deve permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web.
 - 51.3.56.13. Deve permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor web.
 - 51.3.56.14. Deve permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso.
 - 51.3.56.15. A solução deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (rate limit).
 - 51.3.56.16. A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizando mecanismos como HTML Form, Basic e Suporte a SSO, métodos como LDAP e RADIUS para consultas e integração dos usuários da aplicação.
 - 51.3.56.17. Possuir capacidade de caching para aceleração web.

- 51.3.56.18. Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.
- 51.3.56.19. Deve ser capaz de restringir acesso quando as requisições não tiverem um cabeçalho HTTP específico pré-configurado.
- 51.3.56.20. Deve ser capaz de limitar o número de usuários/origens simultâneos acessando a mesma conta/sessão/login.
- 51.3.56.21. Deve ser capaz de criptografar URLs para prevenir acesso forçado e garantir que a estrutura de diretórios interna da aplicação web não seja revelada aos usuários.
- 51.3.56.22. Deve ser capaz de adicionar múltiplos servidores ADFS em um pool de servidores
- 51.3.56.23. Deve implementar recursos de proteção de API (Application Programming Interface) através de Machine learning, implementando a análise dinâmica das chamadas de API para detecção de anomalias e bloqueando ataques direcionados a aplicações baseadas em microserviços.

51.4.FUNCIONALIDADES BALANCEAMENTO DE CARGA

- 51.4.1. A solução deve incluir funcionalidades nativas de balanceamento de carga entre múltiplos servidores web.
- 51.4.2. Deve permitir a configuração de portas não padrão para aplicações HTTP e HTTPS.
- 51.4.3. Deve ser capaz de distribuir o tráfego entre diferentes servidores web e rotear conteúdo de forma inteligente.
- 51.4.4. A solução deve permitir a criação de grupos de servidores (Server Pools/Farms) para distribuição de conexões.
- 51.4.5. Deve suportar a definição de servidores virtuais, com IP e interface de rede/bridge, para recepção do tráfego destinado aos Server Pools.
- 51.4.6. Os servidores virtuais devem encaminhar o tráfego a um servidor específico ou distribuir sessões entre os membros do Pool.
- 51.4.7. Deve ser possível definir o número máximo de conexões TCP simultâneas por servidor membro.
- 51.4.8. A solução deve implementar os seguintes algoritmos de balanceamento de carga: Round Robin, Weighted Round Robin e Least Connections.
- 51.4.9. A solução deve oferecer suporte a testes de disponibilidade de servidores web utilizando os seguintes métodos: TCP, ICMP ECHO_REQUEST (ping), TCP Half Open, TCP SSL, HTTP e HTTPS.
- 51.4.10. Nos testes de disponibilidade via HTTP e HTTPS, a solução deve permitir a definição da

URL exata a ser testada, a escolha do método HTTP (HEAD, GET ou POST) e a configuração do campo "Host" no cabeçalho HTTP.

- 51.4.11. A solução deve suportar o roteamento de requisições com base no conteúdo HTTP, utilizando critérios como: Host, URL, parâmetros HTTP, cabeçalho Referer, endereço IP de origem, cabeçalhos HTTP, cookies e campos do certificado X.509 do cliente.
- 51.4.12. Deve implementar cache de conteúdo para protocolos HTTP, permitindo que objetos sejam armazenados e respostas sejam fornecidas diretamente pela solução.
- 51.4.13. A solução deve suportar persistência de sessão (session stickiness), permitindo o balanceamento de novas conexões enquanto mantém as sessões existentes no mesmo servidor. Devem ser suportados os seguintes métodos: IP de origem, parâmetros do cabeçalho HTTP, URL acessada, cookie insert e cookie rewrite, embedded cookie (cookie original com porção randômica), reescrita de cookie, cookie persistente, ASP Session ID, PHP Session ID, JSP Session ID e sessão SSL.
- 51.4.14. A solução deve ser capaz de retornar código de erro HTTP 503 caso os health-checks estejam desativados ou os servidores de retaguarda estejam indisponíveis.
- 51.4.15. Deve suportar a funcionalidade de marcação de tráfego (FWMARK).

51.5.SERVIÇOS DE GARANTIA TÉCNICA

- 51.5.1. Durante toda a vigência contratual em conjunto com o serviço de garantia técnica oficial do fabricante a CONTRATADA deve prover serviços através de sua própria equipe técnica. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.
- 51.5.2. Em conformidade com a exigência de plantão técnico on-site, a CONTRATADA deve assegurar a disponibilidade de técnicos para deslocamento e atendimento presencial nas dependências das unidades governamentais da Bahia.
- 51.5.3. O atendimento local será acionado sempre que houver perda de conectividade remota com o equipamento ou necessidade de intervenção física (substituição de peças, reconexão de cabos ou restauração de backup via console).
- 51.5.4. Esgotadas as tentativas de solução pela equipe local/remota da revenda, esta terá a obrigação de realizar o escalonamento oficial para a engenharia do fabricante (Vendor Support), mantendo-se responsável pelo acompanhamento do chamado (follow-up) e pela comunicação do status à PRODEB até a resolução definitiva

52.LOTE - 02 - ITEM 27 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAF – TIPO 01

52.1.CARACTERÍSTICAS GERAIS:

- 52.1.1. Licenciamento e serviços de garantia técnica do Fabricante para os equipamentos do ITEM SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAF – TIPO I, pelo período de 12 (doze) meses das funcionalidades: Antivírus, Reputação de IP, Sandbox, Serviço de Defesa de Preenchimento de Credenciais e Análise Avançada de Ameaças.
- 52.1.2. Durante toda a vigência contratual em conjunto com os serviços de garantia técnica oficial do fabricante a CONTRATADA deve prover serviços on site técnico através de sua própria equipe técnica. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.

53.LOTE - 02 - ITEM 28 – SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAF - TIPO 02

53.1.CARACTERÍSTICAS E FUNCIONALIDADES GERAIS

- 53.1.1. A solução deve ser entregue no formato de appliance virtual, compatível com ambientes Amazon AWS, Microsoft Azure, Google GCP, VMware ESXi, Microsoft Hyper-V. A responsabilidade pelo fornecimento e a implantação de servidor/hardware ou recursos computacionais em nuvem será de responsabilidade da CONTRATANTE, e a solução deve ser instalado no ambiente indicado pela CONTRATANTE.
- 53.1.2. Poderá ser feita composição por mais de uma solução para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 53.1.3. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados para funcionar dessa forma.
- 53.1.4. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze) meses, minimamente com as seguintes funcionalidades: Antivírus, Reputação de IP, Sandbox, Serviço de Defesa de Preenchimento de Credenciais e Análise Avançada de Ameaças.
- 53.1.5. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Monitoramento e Relatoria de Logs existente na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F. Caso o item não atenda a esta exigência será preciso entregar solução equivalente de capacidade igual ou superior.

53.2.SERVIÇOS DE GARANTIA TÉCNICA LOCAL

- 53.2.1.1. Durante toda a vigência contratual em conjunto com o suporte técnico oficial do fabricante a CONTRATADA deve prover suporte técnico através de sua própria equipe técnica, o atendimento de primeiro e segundo níveis. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.
- 53.2.1.2. Em conformidade com a exigência de plantão técnico on-site, a CONTRATADA deve assegurar a disponibilidade de técnicos para deslocamento e atendimento presencial nas dependências das unidades governamentais da Bahia.
- 53.2.1.3. O atendimento local será acionado sempre que houver perda de conectividade remota com o equipamento ou necessidade de intervenção física (substituição de peças, reconexão de cabos ou restauração de backup via console).
- 53.2.1.4. Esgotadas as tentativas de solução pela equipe local/remota da revenda, esta terá a obrigação de realizar o escalonamento oficial para a engenharia do fabricante (Vendor Support), mantendo-se responsável pelo acompanhamento do chamado (follow-up) e pela comunicação do status à PRODEB até a resolução definitiva

53.3.REQUISITOS MÍNIMOS DE PERFORMANCE

- 53.3.1. Deve possuir throughput mínimo para HTTP de 500 (quinhentos) Mbps.
- 53.3.2. Deve suportar quantidade ilimitada de aplicações protegidas.

53.4.FUNCIONALIDADES DE REDE

- 53.4.1. A solução deve ser capaz de ser implementada nos modos de operação Proxy Reverso, Proxy Transparente (Inline), Modo Passivo ou Sniffer (Offline), e Bridge Transparente. Deve ainda ser capaz de ser implementada com o protocolo WCCP.
- 53.4.2. Suportar VLANs no padrão IEEE 802.1Q.
- 53.4.3. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP) - IEEE 802.3ad.
- 53.4.4. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs).
- 53.4.5. A solução deve suportar roteamento por política (policy route).

53.5.FUNCIONALIDADES DE GERÊNCIA

- 53.5.1. A solução deve oferecer interface gráfica web (GUI) para configuração e gerenciamento , acessível via navegadores gratuitos utilizando o protocolo HTTPS. Também deve permitir administração via CLI, tanto localmente (porta de console) quanto remotamente via SSH.
- 53.5.2. A interface gráfica deve apresentar informações completas sobre o sistema, incluindo

cluster, hostname, número de série, modo de operação, uptime, versão do firmware, licenciamento, consumo de CPU, memória, estatísticas de conexões, throughput HTTP, requisições, eventos e logs recentes.

- 53.5.3. A administração da solução deve permitir o uso de perfis de acesso.
- 53.5.4. A solução deve permitir backup e restauração pela interface gráfica, com suporte a criptografia e utilização dos protocolos FTP, SFTP, TFTP ou HTTPS.
- 53.5.5. Deve ser possível instalar uma versão alternativa do firmware no disco e inicializá-la manualmente em caso de falha do firmware principal.
- 53.5.6. Deve suportar SNMP (v1, v2c e v3), envio de eventos via e-mail, traps SNMP e Syslog, e armazenar logs localmente e remotamente.
- 53.5.7. A solução deve permitir a adição de identificadores personalizados nos registros Syslog, como o hostname, podendo ser fixos ou variáveis.
- 53.5.8. Deve permitir o envio de alertas por e-mail baseados na severidade e/ou categoria dos eventos.
- 53.5.9. O dashboard deve exibir os últimos logs de ataques detectados ou bloqueados.
- 53.5.10. A interface gráfica deve mostrar o consumo de memória em tempo real.
- 53.5.11. A utilização de disco para armazenamento de logs deve ser acessível via interface gráfica ou CLI.
- 53.5.12. Devem estar disponíveis estatísticas de conexões simultâneas e por segundo, com base nas políticas de segurança.
- 53.5.13. A solução deve exibir estatísticas em tempo real de throughput HTTP, eventos de ataques, requisições HTTP e os últimos eventos do sistema.
- 53.5.14. A interface gráfica deve incluir um painel com informações sobre as interfaces de rede.
- 53.5.15. As informações de licenciamento e assinaturas devem estar disponíveis na interface gráfica.
- 53.5.16. A solução deve oferecer análise geográfica dos acessos web.
- 53.5.17. A solução deve apresentar dados analíticos com total e percentual de ataques, tráfego e acessos (hits), por país de origem.
- 53.5.18. Deve ser possível gerar relatórios detalhados com base em tráfego, acessos e atividades de usuários.
- 53.5.19. A solução deve oferecer suporte a APIs RESTful para gerenciamento de configurações.
- 53.5.20. Deve suportar comunicação com protocolo HTTP/2.

53.6.FUNCIONALIDADES DE AUTENTICAÇÃO

- 53.6.1. A solução deve permitir autenticação de usuários por meio do cabeçalho HTTP/HTTPS Authorization.
- 53.6.2. Deve suportar autenticação via formulários HTML embutidos em páginas web.
- 53.6.3. Deve permitir a autenticação de usuários com uso de certificados digitais pessoais.
- 53.6.4. A solução deve dispor de uma base local para cadastro e autenticação de contas de usuários.
- 53.6.5. Deve ser compatível com autenticação de usuários em diretórios externos, como LDAP e RADIUS.
- 53.6.6. Deve permitir autenticação via NTLM, utilizando contas de usuários armazenadas em servidores remotos.
- 53.6.7. A solução deve possibilitar a criação de grupos de usuários para aplicação de políticas de acesso comuns durante o processo de autenticação.

53.7.FUNCIONALIDADES DE WEB APPLICATION FIREWALL

- 53.7.1. Deve ser capaz de identificar e bloquear ataques através de um banco de dados de assinaturas de vírus e IP reputation, atualizado de forma automática.
- 53.7.2. Deve implementar recursos de Sandbox para análise de malware moderno;
- 53.7.3. Deve implementar recurso de machine learning, onde será permitido implementar proteção para um servidor ou grupo de servidores de aplicação web, de forma automatizada através da análise da utilização da aplicação, fazendo a descoberta da estrutura e padrões e padrões de uso, buscando separar o comportamento anormal do abusivo, detectando anomalias e tentativas de ataque.
- 53.7.4. Deve implementar proteção contra a lista de técnicas/ataques listados no OWASP 10 (Open Web Application security Project)
- 53.7.5. Deve implementar recursos embarcados de antivírus para análise de arquivos, detecção e bloqueio de malwares que possam comprometer os servidores possuindo integração com a nuvem do fabricante para obter atualizações, enviar e receber amostras de malware para análise/verificação.
- 53.7.6. Ter a capacidade de criação de assinaturas de ataque customizáveis.
- 53.7.7. Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol.
- 53.7.8. Ter a capacidade de proteção para ataques do tipo Botnet.
- 53.7.9. Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST).
- 53.7.10. A solução Deve possuir funcionalidade de proteção positiva contra-ataques como acesso

por força bruta.

- 53.7.11. Deve suportar detecção a ataques de Clickjacking.
- 53.7.12. Deve suportar detecção a ataques de alteração de cookie.
- 53.7.13. Deve identificar e prevenir ataques do tipo Credit Card Theft.
- 53.7.14. Deve identificar e prevenir ataques Cross Site Request Forgery (CSRF).
- 53.7.15. A solução deve possuir funcionalidade de proteção positiva contra-ataques como cross site scripting (XSS).
- 53.7.16. Deve possuir proteção contra-ataques de Denial of Service (DoS).
- 53.7.17. Deve possuir a capacidade de proteção para ataques do tipo HTTP header overflow.
- 53.7.18. Deve possuir a capacidade de proteção para ataques do tipo Local File inclusion (FLI).
- 53.7.19. Deve possuir a capacidade de proteção para ataques do tipo Man-in-the-middle (MITM).
- 53.7.20. Deve possuir a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI).
- 53.7.21. Deve possuir a capacidade de proteção para ataques do tipo Server Information Leakage.
- 53.7.22. Deve possuir proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection).
- 53.7.23. Deve possuir a capacidade de proteção para ataques do tipo Malformed XML.
- 53.7.24. Deve Identificar e prevenir ataques do tipo Low-rate DoS.
- 53.7.25. Deve possuir prevenção contra Slow POST attack.
- 53.7.26. Deve proteger contra-ataques Slowloris.
- 53.7.27. Deve possuir a capacidade de proteção para ataques do tipo SYN flood.
- 53.7.28. Deve possuir a capacidade de proteção para ataques do tipo Forms Tampering.
- 53.7.29. A solução deve possuir funcionalidade de proteção positiva contra-ataques de manipulação de campo escondido.
- 53.7.30. Deve possuir a capacidade de proteção para ataques do tipo Directory Traversal.
- 53.7.31. Deve possuir a capacidade de proteção do tipo Access Rate Control.
- 53.7.32. Deve possuir a habilidade de configurar proteção do tipo TCP SYN flood-style para prevenção de DoS para qualquer política, através de Syn Cookie e Half Open Threshold.
- 53.7.33. Deve permitir configurar regras de bloqueio a métodos HTTP indesejados.
- 53.7.34. Deve permitir que sejam configuradas regras de limite de upload por tamanho de arquivo.
- 53.7.35. Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos países, sem a necessidade de gerir manualmente os ranges de endereços IP

correspondentes a cada país.

- 53.7.36. Deve permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem.
- 53.7.37. Deve permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.
- 53.7.38. Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation.
- 53.7.39. Deve possuir a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP.
- 53.7.40. Deve possuir a funcionalidade de proteger o website contra ações de desfiguração (defacement), com restauração automática e rápida do site caso ocorra à falha.
- 53.7.41. Deve possuir a funcionalidade de antivírus para inspeção de tráfego e arquivos.
- 53.7.42. Deve ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia.
- 53.7.43. A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego.
- 53.7.44. Deve para SSL/TLS offload suportar no mínimo TLS 1.0, 1.1, 1.2 e 1.3.
- 53.7.45. A solução deve ter a capacidade de armazenar certificados digitais de CA's.
- 53.7.46. A solução deve ser capaz de gerar CSR para ser assinado por uma CA.
- 53.7.47. A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL).
- 53.7.48. A solução deve conter as assinaturas de robôs conhecidos como link checkers, indexadores de web, search engines, spiders e web crawlers que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões.
- 53.7.49. A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers etc. Tal sistema deve ser atualizado automaticamente.
- 53.7.50. A solução Deve ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores.
- 53.7.51. A solução deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location.
- 53.7.52. A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessadas para prevenir ataques como cross-site request forgery (CSRF).

- 53.7.53. A solução deve ter a capacidade de definir restrições a métodos HTTP.
- 53.7.54. A solução deve ter a capacidade de proteger contra a detecção de campos ocultos.
- 53.7.55. Deve permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares.
- 53.7.56. A solução deve incluir capacidade de atuar como um scanner de vulnerabilidades ou permitir a integração com scanners de vulnerabilidade de terceiros para diagnóstico e identificação de ameaças nos servidores web, software desatualizado e potenciais buffers overflows,
- 53.7.57. Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros.
- 53.7.58. A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML.
- 53.7.59. A solução deve permitir a exclusão de URLs na análise de vulnerabilidades.
- 53.7.60. Deve ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente.
- 53.7.61. Deve suportar redireção e reescrita de requisições e respostas HTTP.
- 53.7.62. Deve permitir redirecionar requisições HTTP para HTTPS.
- 53.7.63. Deve permitir reescrever a linha URL no cabeçalho de uma requisição HTTP.
- 53.7.64. Deve permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP.
- 53.7.65. Deve permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP.
- 53.7.66. Deve permitir redirecionar requisições para outro web site.
- 53.7.67. Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP.
- 53.7.68. Deve permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web.
- 53.7.69. Deve permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor web.
- 53.7.70. Deve permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso.
- 53.7.71. A solução deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (rate limit).
- 53.7.72. A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizando mecanismos como HTML Form, Basic e Suporte a SSO, métodos como LDAP e RADIUS para consultas e integração dos usuários da aplicação.
- 53.7.73. Possuir capacidade de caching para aceleração web.

- 53.7.74. Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.
- 53.7.75. Deve ser capaz de restringir acesso quando as requisições não tiverem um cabeçalho HTTP específico pré-configurado.
- 53.7.76. Deve ser capaz de limitar o número de usuários/origens simultâneos acessando a mesma conta/sessão/login.
- 53.7.77. Deve ser capaz de criptografar URLs para prevenir acesso forçado e garantir que a estrutura de diretórios interna da aplicação web não seja revelada aos usuários.
- 53.7.78. Deve ser capaz de adicionar múltiplos servidores ADFS em um pool de servidores
- 53.7.79. Deve implementar recursos de proteção de API (Application Programming Interface) através de Machine learning, implementando a análise dinâmica das chamadas de API para detecção de anomalias e bloqueando ataques direcionados a aplicações baseadas em microsserviços.

53.8.FUNCIONALIDADES BALANCEAMENTO DE CARGA

- 53.8.1. A solução deve incluir funcionalidades nativas de balanceamento de carga entre múltiplos servidores web.
- 53.8.2. Deve permitir a configuração de portas não padrão para aplicações HTTP e HTTPS.
- 53.8.3. Deve ser capaz de distribuir o tráfego entre diferentes servidores web e rotear conteúdo de forma inteligente.
- 53.8.4. A solução deve permitir a criação de grupos de servidores (Server Pools/Farms) para distribuição de conexões.
- 53.8.5. Deve suportar a definição de servidores virtuais, com IP e interface de rede/bridge, para recepção do tráfego destinado aos Server Pools.
- 53.8.6. Os servidores virtuais devem encaminhar o tráfego a um servidor específico ou distribuir sessões entre os membros do Pool.
- 53.8.7. Deve ser possível definir o número máximo de conexões TCP simultâneas por servidor membro.
- 53.8.8. A solução deve implementar os seguintes algoritmos de balanceamento de carga: Round Robin, Weighted Round Robin e Least Connections.
- 53.8.9. A solução deve oferecer suporte a testes de disponibilidade de servidores web utilizando os seguintes métodos: TCP, ICMP ECHO_REQUEST (ping), TCP Half Open, TCP SSL, HTTP e HTTPS.
- 53.8.10. Nos testes de disponibilidade via HTTP e HTTPS, a solução deve permitir a definição da

URL exata a ser testada, a escolha do método HTTP (HEAD, GET ou POST) e a configuração do campo "Host" no cabeçalho HTTP.

- 53.8.11. A solução deve suportar o roteamento de requisições com base no conteúdo HTTP, utilizando critérios como: Host, URL, parâmetros HTTP, cabeçalho Referer, endereço IP de origem, cabeçalhos HTTP, cookies e campos do certificado X.509 do cliente.
- 53.8.12. Deve implementar cache de conteúdo para protocolos HTTP, permitindo que objetos sejam armazenados e respostas sejam fornecidas diretamente pela solução.
- 53.8.13. A solução deve suportar persistência de sessão (session stickiness), permitindo o balanceamento de novas conexões enquanto mantém as sessões existentes no mesmo servidor. Devem ser suportados os seguintes métodos: IP de origem, parâmetros do cabeçalho HTTP, URL acessada, cookie insert e cookie rewrite, embedded cookie (cookie original com porção randômica), reescrita de cookie, cookie persistente, ASP Session ID, PHP Session ID, JSP Session ID e sessão SSL.
- 53.8.14. A solução deve ser capaz de retornar código de erro HTTP 503 caso os health-checks estejam desativados ou os servidores de retaguarda estejam indisponíveis.
- 53.8.15. Deve suportar a funcionalidade de marcação de tráfego (FWMARK).

54.LOTE - 02 - ITEM 29 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAF – TIPO 02

54.1.CARACTERÍSTICAS GERAIS:

- 54.1.1. Licenciamento e serviços de garantia técnica do Fabricante para os equipamentos do item SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAF – TIPO I, pelo período de 12 (doze) meses das funcionalidades: Antivírus, Reputação de IP, Sandbox, Serviço de Defesa de Preenchimento de Credenciais e Análise Avançada de Ameaças
- 54.1.2. Durante toda a vigência contratual em conjunto com serviços de garantia técnica oficial do fabricante a CONTRATADA deve prover serviços on-site através de sua própria equipe técnica. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.

55.LOTE - 02 - ITEM 30 - SOLUÇÃO DE SEGURANÇA DE REDE NGFW PARA AMBIENTES HÍBRIDOS

- 55.1. A solução deve ser entregue no formato de appliance virtual, compatível com ambientes Amazon AWS, Microsoft Azure, Google GCP, VMware ESXi, Microsoft Hyper-V. A responsabilidade pelo

fornecimento e a implantação de servidor/hardware ou recursos computacionais em nuvem será de responsabilidade da CONTRATANTE, e a solução deve ser instalado no ambiente indicado pela CONTRATANTE.

- 55.2. Poderá ser feita composição por mais de uma solução para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 55.3. A solução deve permitir acesso a gerência e monitoramento, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
- 55.4. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.
- 55.5. Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;
- 55.6. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.
- 55.7. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;
- 55.8. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 55.9. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 55.10. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 2,5 (dois virgula cinco) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou

blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.

55.11. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.

55.12. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

55.13. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

55.14. SUPORTE TECNICO LOCAL

55.14.1. Durante toda a vigência contratual em conjunto com os serviços de garantia técnica oficial do fabricante a CONTRATADA deve prover serviços através de sua própria equipe técnica. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.

55.14.2. Em conformidade com a exigência de plantão técnico on-site, a CONTRATADA deve assegurar a disponibilidade de técnicos para deslocamento e atendimento presencial nas dependências das unidades governamentais da Bahia.

55.14.3. O atendimento local será acionado sempre que houver perda de conectividade remota com o equipamento ou necessidade de intervenção física (substituição de peças, reconexão de cabos ou restauração de backup via console).

55.14.4. Esgotadas as tentativas de solução pela equipe local/remota da revenda, esta terá a obrigação de realizar o escalonamento oficial para a engenharia do fabricante (Vendor Support), mantendo-se responsável pelo acompanhamento do chamado (follow-up) e pela comunicação do status à PRODEB até a resolução definitiva

55.15. FUNCIONALIDADES DE FIREWALL

55.15.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.

55.15.2. Possuir suporte a sub-interfaces ethernet lógicas;

55.15.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.

55.15.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.

- 55.15.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 55.15.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;
- 55.15.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);
- 55.15.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);
- 55.15.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;
- 55.15.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.
- 55.15.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 55.15.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 55.15.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 55.15.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 55.15.15. Deve suportar o encaminhamento de tráfego multicast.
- 55.15.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 55.15.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 55.15.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 55.15.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 55.15.20. Suportar OSPF gracefulrestart;
- 55.15.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 55.15.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 55.15.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 55.15.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 55.15.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e

controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

- 55.15.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 55.15.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 55.15.28. Drop sem notificação do bloqueio ao usuário;
 - 55.15.29. Drop com notificação do bloqueio ao usuário;
 - 55.15.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 55.15.31. TCP-Reset para o cliente;
 - 55.15.32. TCP-Reset para o server ou para os dois lados da conexão.
- 55.15.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 55.15.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 55.15.35. Deve oferecer suporte ao protocolo SIP.
- 55.15.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 55.15.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 55.15.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 55.15.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 55.15.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 55.15.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 55.15.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 55.15.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 55.15.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS

e TACACS +.

- 55.15.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 55.15.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 55.15.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 55.15.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 55.15.49. Realizar Traffic Shaping para a solução de segurança
- 55.15.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 55.15.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 55.15.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 55.15.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 55.15.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 55.15.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 55.15.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 55.15.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 55.15.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 55.15.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 55.15.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;

- 55.15.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 55.15.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 55.15.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 55.15.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 55.15.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 55.15.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 55.15.67. Funcionar com tradução de porta (PAT);
- 55.15.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 55.15.69. Implementar e suportar NAT64 e NAT46;
- 55.15.70. Implementar NAT66
- 55.15.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 55.15.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 55.15.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 55.15.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 55.15.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:
 - 55.15.75.1. Conectores SDN Privados:
 - 55.15.75.1.1. Nutanix;
 - 55.15.75.1.2. Kubernetes;
 - 55.15.75.1.3. VMware ESXi;
 - 55.15.75.1.4. OpenStack;
 - 55.15.75.2. Conectores SDN Públicos;
 - 55.15.75.2.1. Google Cloud Platform (GCP);

55.15.75.2.2. AWS;

55.15.75.2.3. Microsoft Azure;

55.15.75.2.4. Oracle Cloud Infrastructure (OCI);

55.15.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).

55.15.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;

55.15.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).

55.15.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.

55.15.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

55.16. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

55.16.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.

55.16.2. Deve permitir modificação de valores DSCP para o DiffServ.

55.16.3. Deve permitir priorização de tráfego e suportar ToS.

55.16.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.

55.16.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.

55.16.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.

55.16.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.

55.16.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.

55.16.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.

55.16.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP

de origem e destino.

55.17. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

- 55.17.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
- 55.17.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
- 55.17.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
- 55.17.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 55.17.5. Deve permitir a criação de categorias personalizadas.
- 55.17.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 55.17.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 55.17.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 55.17.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 55.17.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 55.17.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 55.17.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 55.17.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 55.17.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 55.17.15. Permitir a criação de categorias de URLs customizadas;
- 55.17.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 55.17.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 55.17.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

- 55.17.19. Permitir a customização de página de bloqueio;
- 55.17.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 55.17.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 55.17.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 55.17.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 55.17.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 55.17.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 55.17.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 55.17.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 55.17.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 55.17.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 55.17.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 55.17.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 55.17.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 55.17.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 55.17.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.

- 55.17.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 55.17.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 55.17.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 55.17.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 55.17.39. Deve possuir Proxy Explícito e Transparente.
- 55.17.40. Deve implementar roteamento WCCP e ICAP.
- 55.18. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)
 - 55.18.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
 - 55.18.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
 - 55.18.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
 - 55.18.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
 - 55.18.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
 - 55.18.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
 - 55.18.7. Deve permitir funcionar em modo transparente, sniffer e router.
 - 55.18.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
 - 55.18.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
 - 55.18.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
 - 55.18.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
 - 55.18.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
 - 55.18.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques,

baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);

- 55.18.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 55.18.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 55.18.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 55.18.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 55.18.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 55.18.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 55.18.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 55.18.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 55.18.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 55.18.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 55.18.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 55.18.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 55.18.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 55.18.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 55.18.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 55.18.29. Identificar, alertar e bloquear comunicação com botnets;
- 55.18.30. Registrar na console de monitoração as seguintes informações sobre ameaças

identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

- 55.18.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 55.18.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 55.18.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 55.18.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 55.18.35. Identificar nos eventos o país de onde partiu a ameaça;
- 55.18.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 55.18.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 55.18.38. Deve possuir alarmes na console de administração.
- 55.18.39. Deve possuir alertas via correio eletrônico.
- 55.18.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 55.18.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 55.18.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 55.18.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 55.18.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;
- 55.19. FUNCIONALIDADE DE VPN
 - 55.19.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
 - 55.19.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
 - 55.19.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption

Standard) 128 ou 256 bits;

- 55.19.4. Suportar nativamente a autenticação de VPN IPsec utilizando MD5 e SHA-1;
 - 55.19.5. Suportar nativamente a criação de VPN IPsec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
 - 55.19.6. Suportar nativamente a criação de VPN IPsec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
 - 55.19.7. Suportar nativamente, para VPN IPsec, autenticação via certificado IKE PKI;
 - 55.19.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPsec a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
 - 55.19.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
 - 55.19.10. Realizar atribuição de DNS nos clientes remotos de VPN;
 - 55.19.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
 - 55.19.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
 - 55.19.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
 - 55.19.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
 - 55.19.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
 - 55.19.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 55.20. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
- 55.20.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
 - 55.20.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não

limitado, o compartilhamento de arquivos;

- 55.20.3. Atualizar a base de assinaturas de aplicações automaticamente;
- 55.20.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
- 55.20.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 55.20.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
- 55.20.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 55.20.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 55.20.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 55.20.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 55.20.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 55.20.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 55.20.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 55.20.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 55.20.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 55.20.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou

transferência de arquivos), etc.

- 55.20.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 55.20.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 55.20.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 55.20.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 55.20.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 55.20.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 55.20.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 55.20.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 55.20.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 55.20.26. Deve permitir criação de padrões de aplicação manualmente.
- 55.20.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 55.20.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 55.20.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 55.20.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;
- 55.21. FUNCIONALIDADE DE SD-WAN
 - 55.21.1. Permitir a utilização de, no mínimo, 04 (quatro) caminhos simultâneos.
 - 55.21.2. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
 - 55.21.3. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
 - 55.21.4. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em

contexto de saída (Nat Outbound) para um pool de IPs públicos;

- 55.21.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
- 55.21.6. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.
- 55.21.7. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/range de IPs de destino;
- 55.21.8. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 55.21.9. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 55.21.10. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 55.21.11. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
 - 55.21.12. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
 - 55.21.13. Passivo: uso do tráfego real para as medições;
 - 55.21.14. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 55.21.15. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 55.21.16. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 55.21.17. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 55.21.18. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um

- destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 55.21.19. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 55.21.20. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 55.21.21. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 55.21.22. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 55.21.23. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 55.21.24. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 55.21.25. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 55.21.26. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 55.21.27. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;
- 55.22. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE
- 55.22.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração, incluindo:
- 55.22.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.
- 55.22.1.2. Execução de testes operacionais e validação do funcionamento da solução antes da

entrega formal à CONTRATANTE.

55.22.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:

55.22.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.

55.22.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.

55.22.2.3. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

56.LOTE - 02 - ITEM 31 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE SEGURANÇA DE REDE NGFW PARA AMBIENTES HÍBRIDOS

56.1.CARACTERÍSTICAS GERAIS:

56.1.1. Licenciamento e serviços de garantia técnica do Fabricante para o ITEM SOLUÇÃO DE SEGURANÇA DE REDE NGFW PARA AMBIENTES HÍBRIDOS, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN.

56.1.2. Durante toda a vigência contratual em conjunto com os serviços de garantia técnica oficial do fabricante a CONTRATADA deve prover serviços on-site através de sua própria equipe técnica. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.

57.LOTE - 02 - ITEM 32 – SOLUÇÃO DE SEGURANÇA DECOY/HONEYPOT

57.1.A solução deve ser entregue no formato de appliance virtual, compatível com ambientes Amazon AWS, Microsoft Azure, Google GCP, VMware ESXi, Microsoft Hyper-V. A responsabilidade pelo fornecimento e a implantação de servidor/hardware ou recursos computacionais em nuvem será de responsabilidade da CONTRATANTE, e a solução deve ser instalado no ambiente indicado pela CONTRATANTE.

57.2.Deve possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 12 (doze) meses.

- 57.3. Poderá ser feita composição por mais de uma solução para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 57.4. Deve suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções
- 57.5. Deve ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.
- 57.6. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de existente na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 57.7. Deve suportar ter a capacidade mínima de 10 VM de honeypot;
- 57.8. Deve suportar no mínimo 120 VLAN's e estar licenciado para no mínimo 05 VLAN's ou ou 5 redes distintas por barramento prefixo /24 (255.255.255.0) ou maior (/25, /26, /27, etc...);;
- 57.9. Deve possuir 02 (dois) licenciamento incluso de Windows 7 ou superior.
- 57.10. Deve possuir licenciamento pelo período de 12 (doze) meses para as funcionalidades de Deception Decoys, AV, IPS, e Web Filtering;
- 57.11. Deve suportar a seguinte combinação:
- 57.11.1. Windows 7, Windows 10, Windows 10 (customizable BYOL), Windows Server 2016 and 2019 ou superior
 - 57.11.2. Linux, VPN Server
 - 57.11.3. Medical (PACS, Infusion pump), ERP
 - 57.11.4. IoT, SAP and/or SCADA
- 57.12. Deve suportar os seguintes serviços:
- 57.12.1. SSH, SAMBA, SMB, RDP, HTTP/S, SQL, GIT, DICOM, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, EtherNet/IP, DNP3, JET-DIRECT, RTSP, UPnP, TCP port listener
- 57.13. Deve ser capaz de criar uma rede de máquinas virtuais que se comportam como dispositivos reais a fim de atrair invasores e monitorar suas atividades na rede.
- 57.14. Deve ser capaz de monitorar as ações de atacantes que tentem violar as máquinas virtuais.
- 57.15. Deve analisar as ações dos invasores ao tentarem invadir as máquinas virtuais.
- 57.16. Deve ser capaz de simular serviços, aplicativos ou usuários nas máquinas virtuais a fim de simular um ambiente corporativo real.
- 57.17. Deve possibilitar a instalação de pacote ou script em endpoints reais que simulem

interação com os serviços das máquinas virtuais a fim de influenciar o comportamento dos atacantes aumentando a superfície de engano.

- 57.18. O administrador deve ser capaz de monitorar ataques através de incidentes, lista de ataques e por representação visual da rede mostrando endpoints, máquinas virtuais do dispositivo e ataques em andamento.
- 57.19. O sistema deve ser capaz de demonstrar o número de incidentes por tipo de serviço abrangendo minimamente os seguintes: SSH, SAMBA, SMB, RDP, HTTP, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST e IEC104.
- 57.20. Deve suportar a criação de perfis de administrador para controlar os privilégios de acesso aos recursos do sistema. Ao criar uma conta de administrador deve ser atribuído um perfil à conta;
- 57.21. Deve possuir minimamente os seguintes perfis de administrador: super admin - tendo acesso a todas as funcionalidades e read only - tendo acesso somente leitura. Adicionalmente deve possibilitar a criação e customização de perfis administrativos;
- 57.22. Deve suportar a autenticação remota de administradores usando servidores RADIUS e LDAP;
- 57.23. Deve ser capaz de ser implantado em redes do tipo offline ou air-gapped
- 57.24. Deve permitir inserir a licença de uso do equipamento mesmo em redes do tipo offline ou air-gapped
- 57.25. Deve ser capaz de atualizar o firmware mesmo em redes do tipo offline ou air-gapped;
- 57.26. Deve ser capaz de atualizar o módulo de segurança mesmo em redes do tipo offline ou air-gapped;
- 57.27. Deve ser capaz de armazenar Log no próprio equipamento ou integrar com um servidor remoto de armazenamento de log;
- 57.28. Deve suportar servidor de log remoto do tipo syslog e CEF.
- 57.29. Deve possuir dashboard que mostre informações dos seguintes itens:
- 57.30. Informações do sistema como: Hostname, versão do firmware e usuário conectado no momento;
- 57.31. Número de incidente e eventos com seus níveis de severidade por intervalo de tempo;
- 57.32. Número de decoy implementado;
- 57.33. Performance de CPU e RAM;
- 57.34. Informação de uso de disco;
- 57.35. Widget de Top attack;

- 57.36. Deve ser capaz de customizar o dashboard;
- 57.37. Deve ser capaz de atualizar o firmware via interface gráfica;
- 57.38. Deve ser capaz de realizar o backup e restore via interface gráfica;
- 57.39. Deve ser capaz de configurar rotas (camada 3 OSI);
- 57.40. Deve suportar configuração de cliente DNS;
- 57.41. Deve suportar configuração de IPv4 e IPv6;
- 57.42. Deve ser capaz de criar diferentes perfis de conta de administrador do sistema;
- 57.43. Deve ser capaz de integrar com servidor LDAP e Radius;
- 57.44. Deve suportar a importação de certificados CA;
- 57.45. Deve suportar a configuração de cliente de e-mail para envio de alertas;
- 57.46. Deve ser capaz de escolher o nível de severidade do alerta que será enviado;
- 57.47. Deve suportar SNMP V1, V2 e V3;
- 57.48. Deve suportar conexão com a base de dados do fabricante para atualizar informações de segurança;
- 57.49. Deve suportar integração com sistema de detecção de malware;
- 57.50. Deve suportar integração com SandBox
- 57.51. Deve suportar integração com NGFW do mesmo fabricante ou de terceiros;
- 57.52. Quando integrado com solução de NGFW deve permitir:
- 57.53. Quarentenar dispositivos;
- 57.54. Exibir o status de IP bloqueado;
- 57.55. Exportar arquivo IOC no formato CSV ou STIX;
- 57.56. Mitigar e isolar de forma automática endpoint infectado para prevenir ataques ou movimentação lateral na rede;
- 57.57. Deve ser capaz de listar os incidentes detectados com no mínimo a informação de: severidade, protocolo, tipo, IP do invasor, IP da vítima, ID do Decoy, usuário invasor, porta de origem do ataque, data e hora do ataque;
- 57.58. Deve ser capaz de gerar relatórios em PDF ou CSV;
- 57.59. Deve ser capaz de listar os ataques detectados com as informações de severidade, data e hora, informação do IP do atacante;
- 57.60. Deve ser capaz de montar uma representação da rede em forma de mapa contendo informação do endpoint, decoy e ataque;
- 57.61. Deve ser capaz de classificar o nível de risco dos incidentes e eventos;
- 57.62. Deve ser capaz de informar a quantidade de eventos e incidentes que ocorreram em

uma faixa de tempo;

- 57.63. Deve ser capaz de listar pelo menos o top 5 atacantes;
- 57.64. Deve ser capaz de listar o número de incidente por serviço de forma gráfica;
- 57.65. Deve ser capaz de implantar VMs Decoy na rede, para monitorar e ajudar a entender as ações de um atacante ao obter acesso não autorizado ao Decoy;
- 57.66. Deve ser capaz de implementar decoy customizado (custom image);
- 57.67. Deve suportar importação de imagem ISO;
- 57.68. Deve ser capaz de customizar o recuso de CPU, Memória e Armazenamento da VM-decoy;

57.69. SERVIÇOS DE GARANTIA TÉCNICA LOCAL

- 57.69.1. Durante toda a vigência contratual em conjunto com Os serviços de garantia técnica oficial do fabricante a CONTRATADA deve prover serviços através de sua própria equipe técnica, o atendimento de primeiro e segundo níveis. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.
- 57.69.2. Em conformidade com a exigência de plantão técnico on-site, a CONTRATADA deve assegurar a disponibilidade de técnicos para deslocamento e atendimento presencial nas dependências das unidades governamentais da Bahia.
- 57.69.3. O atendimento local será acionado sempre que houver perda de conectividade remota com o equipamento ou necessidade de intervenção física (substituição de peças, reconexão de cabos ou restauração de backup via console).
- 57.69.4. Esgotadas as tentativas de solução pela equipe local/remota da revenda, esta terá a obrigação de realizar o escalonamento oficial para a engenharia do fabricante (Vendor Support), mantendo-se responsável pelo acompanhamento do chamado (follow-up) e pela comunicação do status à PRODEB até a resolução definitiva

58.LOTE - 02 - ITEM 33 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE SEGURANÇA DECOY/HONEYPOT

58.1.CARACTERÍSTICAS GERAIS:

- 58.1.1. Licenciamento e serviços de garantia técnica do Fabricante para o ITEM SOLUÇÃO DE SEGURANÇA DECOY/HONEYPOT, pelo período de 12 (doze) meses das funcionalidades: no mínimo 10 VM de honeypot e 05 VLAN's.
- 58.1.2. Durante toda a vigência contratual em conjunto com os serviços de garantia técnica

oficial do fabricante a CONTRATADA deve prover serviços on-site através de sua própria equipe técnica. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.

59.LOTE - 02 - ITEM 34 - SOLUÇÃO DE SEGURANÇA DE REDE NGFW – TIPO 02

- 59.1. A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.
- 59.2. Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma arquitetura específica e dedicada (appliance físico), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;
- 59.3. A solução poderá ser composta por mais de um equipamento para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.
- 59.4. A solução deve permitir acesso a gerência e monitoramento, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);
- 59.5. A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.
- 59.6. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.
- 59.7. Deve suportar e estar licenciado para a criação de, ao menos, 10 (dez) instâncias virtuais de firewall no mesmo hardware.
- 59.8. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados

diferentemente;

- 59.9. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.
- 59.10. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 59.11. Deve possuir fonte de alimentação com chaveamento automático 110/220V.
- 59.12. Deve possuir firewall com capacidade mínima de processamento de 6 (seis) Gbps.
- 59.12.1. Deve possuir IPS com capacidade mínima de processamento de 1 (um) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 59.13. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1,2 (um virgula dois) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 59.14. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 1,3 (um virgula três) Gbps.
- 59.15. Deve possuir VPN com capacidade de, pelo menos, 06 (seis) Gbps de tráfego IPsec.
- 59.16. Deve suportar 1.000.000 (um milhão) conexões simultâneas.
- 59.17. Deve suportar, pelo menos, 100.000 (cem mil) novas conexões por segundo.
- 59.18. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.
- 59.19. Deve suportar, pelo menos, 450 (quatrocentos e cinquenta) túneis de VPN Client-Site.
- 59.20. Deve possuir, pelo menos, 09 (nove) interfaces RJ45 1GE.
- 59.21. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 59.22. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

59.23. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

59.24. SERVIÇO DE GARANTIA TÉCNICA LOCAL

59.24.1. Durante toda a vigência contratual em conjunto com os serviços de garantia técnica oficial do fabricante a CONTRATADA deve prover serviços através de sua própria equipe técnica. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.

59.24.2. Em conformidade com a exigência de plantão técnico on-site, a CONTRATADA deve assegurar a disponibilidade de técnicos para deslocamento e atendimento presencial nas dependências das unidades governamentais da Bahia.

59.24.3. O atendimento local será acionado sempre que houver perda de conectividade remota com o equipamento ou necessidade de intervenção física (substituição de peças, reconexão de cabos ou restauração de backup via console).

59.24.4. Esgotadas as tentativas de solução pela equipe local/remota da revenda, esta terá a obrigação de realizar o escalonamento oficial para a engenharia do fabricante (Vendor Support), mantendo-se responsável pelo acompanhamento do chamado (follow-up) e pela comunicação do status à PRODEB até a resolução definitiva

59.25. FUNCIONALIDADES DE FIREWALL

59.25.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.

59.25.2. Possuir suporte a sub-interfaces ethernet lógicas;

59.25.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.

59.25.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.

59.25.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

59.25.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;

59.25.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);

59.25.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);

59.25.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;

59.25.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões

previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.

- 59.25.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.
- 59.25.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 59.25.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 59.25.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 59.25.15. Deve suportar o encaminhamento de tráfego multicast.
- 59.25.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 59.25.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 59.25.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 59.25.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 59.25.20. Suportar OSPF gracefulstart;
- 59.25.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 59.25.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 59.25.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 59.25.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 59.25.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 59.25.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 59.25.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 59.25.28. Drop sem notificação do bloqueio ao usuário;
 - 59.25.29. Drop com notificação do bloqueio ao usuário;
 - 59.25.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 59.25.31. TCP-Reset para o cliente;
 - 59.25.32. TCP-Reset para o server ou para os dois lados da conexão.

- 59.25.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 59.25.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 59.25.35. Deve oferecer suporte ao protocolo SIP.
- 59.25.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 59.25.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 59.25.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 59.25.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 59.25.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 59.25.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 59.25.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 59.25.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 59.25.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 59.25.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 59.25.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 59.25.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;

- 59.25.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 59.25.49. Realizar Traffic Shaping para a solução de segurança
- 59.25.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 59.25.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 59.25.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 59.25.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 59.25.54. 2.9.6. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 59.25.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 59.25.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 59.25.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 59.25.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 59.25.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 59.25.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 59.25.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 59.25.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 59.25.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 59.25.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 59.25.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 59.25.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 59.25.67. Funcionar com tradução de porta (PAT);

- 59.25.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 59.25.69. Implementar e suportar NAT64 e NAT46;
- 59.25.70. Implementar NAT66
- 59.25.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 59.25.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 59.25.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 59.25.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 59.25.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:
 - 59.25.75.1. Conectores SDN Privados:
 - 59.25.75.1.1. Nutanix;
 - 59.25.75.1.2. Kubernetes;
 - 59.25.75.1.3. VMware ESXi;
 - 59.25.75.1.4. OpenStack;
 - 59.25.75.2. Conectores SDN Públicos:
 - 59.25.75.2.1. Google Cloud Platform (GCP);
 - 59.25.75.2.2. AWS;
 - 59.25.75.2.3. Microsoft Azure;
 - 59.25.75.2.4. Oracle Cloud Infrastructure (OCI);
- 59.25.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 59.25.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 59.25.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).

59.25.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.

59.25.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento, com acesso protegido por usuário e senha.

59.26. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

59.26.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.

59.26.2. Deve permitir modificação de valores DSCP para o DiffServ.

59.26.3. Deve permitir priorização de tráfego e suportar ToS.

59.26.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.

59.26.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.

59.26.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.

59.26.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.

59.26.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.

59.26.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.

59.26.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

59.27. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

59.27.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.

59.27.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.

59.27.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.

59.27.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

59.27.5. Deve permitir a criação de categorias personalizadas.

59.27.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.

- 59.27.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.
- 59.27.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 59.27.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 59.27.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 59.27.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 59.27.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 59.27.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 59.27.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 59.27.15. Permitir a criação de categorias de URLs customizadas;
- 59.27.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 59.27.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 59.27.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 59.27.19. Permitir a customização de página de bloqueio;
- 59.27.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 59.27.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 59.27.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

- 59.27.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 59.27.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em políticas definidas pela CONTRATANTE aderente;
- 59.27.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 59.27.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 59.27.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 59.27.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 59.27.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 59.27.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 59.27.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 59.27.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 59.27.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 59.27.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 59.27.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 59.27.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 59.27.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 59.27.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 59.27.39. Deve possuir Proxy Explícito e Transparente.
- 59.27.40. Deve implementar roteamento WCCP e ICAP.
- 59.28. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)
 - 59.28.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e

porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.

- 59.28.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.
- 59.28.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 59.28.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 59.28.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 59.28.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 59.28.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 59.28.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 59.28.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 59.28.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 59.28.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 59.28.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 59.28.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 59.28.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 59.28.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 59.28.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 59.28.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias,

como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.

- 59.28.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).
- 59.28.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 59.28.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 59.28.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 59.28.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 59.28.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 59.28.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 59.28.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 59.28.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 59.28.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 59.28.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 59.28.29. Identificar, alertar e bloquear comunicação com botnets;
- 59.28.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 59.28.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 59.28.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 59.28.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim

- como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 59.28.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
 - 59.28.35. Identificar nos eventos o país de onde partiu a ameaça;
 - 59.28.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
 - 59.28.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
 - 59.28.38. Deve possuir alarmes na console de administração.
 - 59.28.39. Deve possuir alertas via correio eletrônico.
 - 59.28.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
 - 59.28.41. Deve ter a capacidade de resposta/logs ativa a ataques.
 - 59.28.42. Incluir proteção contra ataques de negação de serviços (DoS);
 - 59.28.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
 - 59.28.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;
- 59.29. FUNCIONALIDADE DE VPN
- 59.29.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
 - 59.29.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
 - 59.29.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
 - 59.29.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
 - 59.29.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
 - 59.29.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
 - 59.29.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
 - 59.29.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);

- 59.29.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
- 59.29.10. Realizar atribuição de DNS nos clientes remotos de VPN;
- 59.29.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 59.29.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 59.29.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 59.29.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 59.29.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 59.29.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 59.29.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPsec estabelecidos.
- 59.30. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
 - 59.30.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
 - 59.30.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
 - 59.30.3. Atualizar a base de assinaturas de aplicações automaticamente;
 - 59.30.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
 - 59.30.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
 - 59.30.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;

- 59.30.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;
- 59.30.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 59.30.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 59.30.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 59.30.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 59.30.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 59.30.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 59.30.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 59.30.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 59.30.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 59.30.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 59.30.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 59.30.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 59.30.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no

Microsoft Active Directory.

- 59.30.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.
- 59.30.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 59.30.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 59.30.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 59.30.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 59.30.26. Deve permitir criação de padrões de aplicação manualmente.
- 59.30.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 59.30.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 59.30.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 59.30.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;
- 59.31. FUNCIONALIDADE DE SD-WAN
 - 59.31.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
 - 59.31.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.
 - 59.31.2.1. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
 - 59.31.2.2. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
 - 59.31.2.3. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
 - 59.31.2.4. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e

reconhecimento em camada 7 de aplicações;

59.31.2.5. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.

59.31.2.6. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino;

59.31.2.7. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;

59.31.2.8. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

59.31.2.9. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.

59.31.2.10. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:

59.31.2.11. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;

59.31.2.12. Passivo: uso do tráfego real para as medições;

59.31.2.13. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.

59.31.2.14. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;

59.31.2.15. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.

59.31.2.16. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

59.31.2.17. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold

para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;

- 59.31.2.18. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 59.31.2.19. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o objetivo de bloquear malwares e identificar aplicações em camada 7.
- 59.31.2.20. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 59.31.2.21. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 59.31.2.22. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 59.31.2.23. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 59.31.2.24. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 59.31.2.25. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 59.31.2.26. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 59.31.2.27. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;
- 59.32. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE

59.32.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:

59.32.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.

59.32.1.2. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.

59.32.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:

59.32.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Gerenciamento de Dispositivos.

59.32.2.2. Envio contínuo de logs para a Solução de gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.

59.32.2.3. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

60.LOTE - 02 - ITEM 35 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE SEGURANÇA DE REDE NGFW – TIPO 02

60.1.CARACTERÍSTICAS GERAIS:

60.1.1. Licenciamento e serviços de garantia técnico do Fabricante para o ITEM SOLUÇÃO DE SEGURANÇA DE REDE NGFW – TIPO II, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.

60.1.2. Durante toda a vigência contratual em conjunto com serviços de garantia técnica oficial do fabricante a CONTRATADA deve prover serviços on-site através de sua própria equipe técnica. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.

61.LOTE - 02 - ITEM 36 - SOLUÇÃO DE SEGURANÇA DE REDE NGFW – TIPO 03

61.1.A solução deverá ser baseada em appliance físico. Para garantir maior segurança, não serão aceitos equipamentos de uso genérico (como PCs ou servidores convencionais) que permitam a instalação e/ou execução de sistemas operacionais de propósito geral, tais como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS X ou distribuições GNU/Linux.

61.2.Os equipamentos fornecidos para a solução da funcionalidade de segurança devem ter uma

arquitetura específica e dedicada (appliance físico), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;

61.3.A solução poderá ser composta por mais de um equipamento para atender às funcionalidades exigidas, desde que todos os componentes sejam do mesmo fabricante, garantindo total compatibilidade e integração.

61.4.A solução deve permitir acesso a gerência e monitoramento, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);

61.5.A solução deve suportar configuração de cluster em modos de alta disponibilidade ATIVO-ATIVO e ATIVO-PASSIVO. Todos os equipamentos que compõem a solução devem ser compatíveis com esses modos de operação e estar devidamente licenciados de maneira integral e independente do modo de operação, seja em cluster de alta disponibilidade ou standalone. Não serão aceitos programas de licenciamento individual que contemplem apenas os equipamentos operando em alta disponibilidade.

61.6.Possuir módulos de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall;

61.7.Deve possuir e estar licenciado durante a vigência contratual de 12 (doze) meses, minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN, Controle de Aplicações e virtualização de instâncias de firewall por contextos de segurança.

61.7.1. Deve suportar e estar licenciado para a criação de, ao menos 10(dez) instâncias virtuais de firewall no mesmo hardware.

61.7.2. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados diferentemente;

61.7.3. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

61.7.4. Possuir controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

61.7.5. Deve possuir fonte de alimentação com chaveamento automático 110/220V.

61.7.6. Deve possuir firewall com capacidade mínima de processamento de 26 (vinte e seis)

Gbps.

- 61.7.7. Deve possuir IPS com capacidade mínima de processamento de 5 (cinco) Gbps. Para efeitos de comprovação pode também ser considerado o throughput de Threat Protection.
- 61.7.8. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 2,5 (dois vírgula cinco) Gbps. O desempenho exigido de proteção contra ameaças avançadas deverá ser considerando os recursos de controle de aplicação, IPS, proteção contra malware e antivírus habilitados simultaneamente, considerando tráfego enterprise mix ou blend de protocolos/tamanho de pacote/tráfego. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito. Os números devem ser comprovados com documentação pública, disponível no site do fabricante.
- 61.7.9. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 3 (três) Gbps.
- 61.7.10. Deve possuir VPN com capacidade de, pelo menos, 33 (trinta e três) Gbps de tráfego IPSec.
- 61.7.11. Deve suportar 3.000.000 (três milhões) conexões simultâneas.
- 61.7.12. Deve suportar, pelo menos, 135.000 (cento e trinta e cinco mil) novas conexões por segundo.
- 61.7.13. Deve suportar, pelo menos, 1800 (mil e oitocentos) túneis de VPN Site-Site.
- 61.7.14. Deve suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site.
- 61.7.15. Deve possuir, pelo menos, 10 (dez) interfaces RJ45 1GE.
- 61.7.16. Deve possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE.
- 61.7.17. Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.
- 61.8. Deve ser integrável, garantindo o uso pleno das funcionalidades da atual Solução de Relatoria de Logs e a Solução de Gerenciamento Centralizado existentes na PRODEB, Marca Fortinet, Modelo FortiAnalyzer FG3700F e FortiManager FG3000G. Caso o item não atenda a esta exigência será preciso entregar soluções equivalentes de capacidade igual ou superior.
- 61.9. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.
- 61.10. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.
- 61.11. SUPORTE TECNICO LOCAL
 - 61.11.1. Durante toda a vigência contratual em conjunto com o suporte técnico oficial do

fabricante a CONTRATADA deve prover suporte técnico através de sua própria equipe técnica, o atendimento de primeiro e segundo níveis. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.

61.11.2. Em conformidade com a exigência de plantão técnico on-site, a CONTRATADA deve assegurar a disponibilidade de técnicos para deslocamento e atendimento presencial nas dependências das unidades governamentais da Bahia.

61.11.3. O atendimento local será acionado sempre que houver perda de conectividade remota com o equipamento ou necessidade de intervenção física (substituição de peças, reconexão de cabos ou restauração de backup via console).

61.11.4. Esgotadas as tentativas de solução pela equipe local/remota da revenda, esta terá a obrigação de realizar o escalonamento oficial para a engenharia do fabricante (Vendor Support), mantendo-se responsável pelo acompanhamento do chamado (follow-up) e pela comunicação do status à PRODEB até a resolução definitiva

61.12. FUNCIONALIDADES DE FIREWALL

61.12.1. Deve suportar o uso de tags de VLAN conforme o padrão IEEE 802.1Q.

61.12.2. Possuir suporte a sub-interfaces ethernet lógicas;

61.12.3. Deve permitir operação nos modos bridge (sem alterar o endereço MAC dos pacotes trafegados), roteador, proxy explícito e sniffer.

61.12.4. Deve permitir a aplicação de filtros de pacotes mesmo quando operando em camada 2.

61.12.5. Realizar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

61.12.6. Realizar controle de políticas por usuários, grupos de usuários, endereços IPs, redes e zonas de segurança;

61.12.7. Realizar controle de políticas por código de País (por exemplo: BR, USA, UK, RUS);

61.12.8. Criar políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja(m) bloqueado(s);

61.12.9. Realizar a visualização dos países de origem e destino nos logs dos acessos;

61.12.10. Realizar a criação de regiões geográficas, caso a solução não forneça as regiões previamente cadastradas, pela interface gráfica e criar políticas utilizando as mesmas.

61.12.11. Deve permitir o encaminhamento (forwarding) de tráfego em camada 2 para protocolos não baseados em IP.

- 61.12.12. Realizar controle, inspeção e de-criptografia de SSL por política, para tráfego de entrada (Inbound) e saída (Outbound);
- 61.12.13. De-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.3;
- 61.12.14. Decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 61.12.15. Deve suportar o encaminhamento de tráfego multicast.
- 61.12.16. Deve suportar os protocolos de roteamento multicast PIM Sparse Mode e PIM Dense Mode.
- 61.12.17. Implementar objetos e regras, inclusive para protocolos de roteamento multicast;
- 61.12.18. Realizar, para IPv4, roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 61.12.19. Realizar, para IPv6, roteamento estático e dinâmico (OSPFv3 e BGPv4);
- 61.12.20. Suportar OSPF gracefulrestart;
- 61.12.21. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 61.12.22. Deve suportar o uso de roteamento baseado em políticas (PBR – Policy Based Routing).
- 61.12.23. Ter a capacidade de operar de forma simultânea em uma única instância de Firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
- 61.12.24. Suportar Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
- 61.12.25. 2.2.25. Suportar Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
- 61.12.26. Suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 61.12.27. Realizar no mínimo três dos seguintes tipos de negação de tráfego nas políticas de Firewall:
 - 61.12.28. Drop sem notificação do bloqueio ao usuário;
 - 61.12.29. Drop com notificação do bloqueio ao usuário;
 - 61.12.30. Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego;
 - 61.12.31. TCP-Reset para o cliente;
 - 61.12.32. TCP-Reset para o server ou para os dois lados da conexão.
- 61.12.33. Realizar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- 61.12.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos

Firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via webhooks e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

- 61.12.35. Deve oferecer suporte ao protocolo SIP.
- 61.12.36. Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow.
- 61.12.37. Deve permitir a definição de serviços com base em portas ou conjunto de portas dos protocolos TCP, UDP, ICMP e IP.
- 61.12.38. Deve permitir o agrupamento de serviços para facilitar a aplicação de regras.
- 61.12.39. Deve permitir a abertura dinâmica de portas por fluxo de dados para aplicações que utilizem portas variáveis.
- 61.12.40. Deve permitir a criação de regras com base em usuário, grupo de usuários, endereços IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação.
- 61.12.41. Deve permitir o controle de acesso à internet com base em períodos do dia e dias da semana, possibilitando políticas por horário.
- 61.12.42. Deve permitir o controle de acesso à internet por domínio, como por exemplo: gov.br, org.br, edu.br.
- 61.12.43. Deve permitir o controle de acesso à internet com base em endereços IP de origem e destino.
- 61.12.44. Deve permitir autenticação de usuários utilizando base local, servidores LDAP, RADIUS e TACACS +.
- 61.12.45. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 61.12.46. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 61.12.47. Possuir a capacidade de identificar usuários de rede com integração ao LDAP e LDAP/AD, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários;
- 61.12.48. Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do LDAP, LDAP/AD;
- 61.12.49. Realizar Traffic Shaping para a solução de segurança

- 61.12.50. Criar políticas de QoS e Traffic Shaping por endereço de origem e destino;
- 61.12.51. Realizar a criação de políticas de QoS e Traffic Shaping por porta;
- 61.12.52. Realizar pelo QoS a definição de classes por banda garantida, por banda máxima e por fila de prioridade;
- 61.12.53. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping, em modo web ou CLI (Command Line Interface);
- 61.12.54. Realizar QoS (Traffic Shapping) em interface agregadas ou redundantes.
- 61.12.55. Deve possuir integração com soluções de autenticação em dois fatores (2FA) utilizando tokens.
- 61.12.56. Deve suportar autenticação transparente (Single Sign-On) com Active Directory e RADIUS.
- 61.12.57. Permitir na solução monitorar falhas de hardware, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 61.12.58. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 61.12.59. A solução de Firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, mac address, hashes de malwares e domínios;
- 61.12.60. Deve identificar arquivos compactados e aplicar políticas sobre o conteúdo desses tipos de arquivos;
- 61.12.61. Deve identificar arquivos e aplicar políticas sobre esses tipos de arquivos;
- 61.12.62. Deve permitir o vínculo entre endereços IP e MAC (IP/MAC binding), garantindo maior controle sobre a rede interna e prevenindo ataques de IP spoofing.
- 61.12.63. Deve possuir mecanismos de proteção contra spoofing de endereços (anti-spoofing).
- 61.12.64. Deve oferecer mecanismos de tratamento (session-helpers ou ALGs) para protocolos e aplicações.
- 61.12.65. Funcionar com tradução de endereços de rede (NAT) dinâmico (Many-to-1 e Many-to-Many);
- 61.12.66. Funcionar com NAT estático (1-to-1, Many-to-Many, bidirecional 1-to-1);
- 61.12.67. Funcionar com tradução de porta (PAT);
- 61.12.68. Funcionar com NAT de Origem e NAT de Destino simultaneamente;
- 61.12.69. Implementar e suportar NAT64 e NAT46;
- 61.12.70. Implementar NAT66

- 61.12.71. Deve possuir funcionalidades de servidor DHCP, cliente DHCP e relay DHCP.
- 61.12.72. Deve oferecer funcionalidade de balanceamento de carga e contingência de múltiplos links WAN.
- 61.12.73. Deve suportar configuração de alta disponibilidade (HA) nos modos Ativo-Ativo e Ativo-Passivo, com divisão de carga e todas as licenças necessárias ativadas, sem interrupção das conexões.
- 61.12.74. Deve suportar o uso de certificados digitais no padrão X.509, bem como os protocolos SCEP, geração de CSR (Certificate Signing Request) e verificação OCSP.
- 61.12.75. Possuir conectores de SDN (Software-Defined Networking) com nuvens públicas e privadas. Esses conectores devem permitir que mudanças dinâmicas nos atributos do ambiente de nuvem sejam automaticamente atualizadas nos dispositivos CPE DE CONECTIVIDADE SEGURA como objetos de endereços os quais possam ser utilizados em políticas de Firewall. Devendo ser compatível com pelo menos 5 dos conectores abaixo:
 - 61.12.75.1. Conectores SDN Privados:
 - 61.12.75.1.1. Nutanix;
 - 61.12.75.1.2. Kubernetes;
 - 61.12.75.1.3. VMware ESXi;
 - 61.12.75.1.4. OpenStack;
 - 61.12.75.2. Conectores SDN Públicos;
 - 61.12.75.2.1. Google Cloud Platform (GCP);
 - 61.12.75.2.2. AWS;
 - 61.12.75.2.3. Microsoft Azure;
 - 61.12.75.2.4. Oracle Cloud Infrastructure (OCI);
- 61.12.76. Deve permitir que comunicação entre a estação de gerenciamento e o equipamento (appliance) seja criptografada, tanto via interface gráfica quanto via CLI (linha de comando).
- 61.12.77. Garantir que o gerenciamento da solução suporte acesso por, no mínimo, duas das seguintes formas: SSH e WEB (HTTPS), devendo também garantir o acesso via base de usuários LDAP e LDAP/AD;
- 61.12.78. O dispositivo deve contar com técnicas de detecção de softwares de compartilhamento de arquivos (P2P) e de mensagens instantâneas (IM).
- 61.12.79. Deve permitir a criação e agrupamento de objetos de usuários, redes, FQDNs, protocolos e serviços, para simplificar a aplicação de regras.
- 61.12.80. Deve dispor de porta serial ou USB para testes e configuração local do equipamento,

com acesso protegido por usuário e senha.

61.13. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

- 61.13.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS.
- 61.13.2. Deve permitir modificação de valores DSCP para o DiffServ.
- 61.13.3. Deve permitir priorização de tráfego e suportar ToS.
- 61.13.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web.
- 61.13.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 61.13.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP.
- 61.13.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP.
- 61.13.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação.
- 61.13.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino.
- 61.13.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

61.14. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

- 61.14.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança.
- 61.14.2. Deve possuir a funcionalidade de cota de tempo de utilização por categoria.
- 61.14.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como: Proxy anônimo, Webmail, Instituições de saúde, Notícias, Phishing, Hackers, Pornografia, Racismo, Websites pessoais, Compras.
- 61.14.4. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.
- 61.14.5. Deve permitir a criação de categorias personalizadas.
- 61.14.6. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP.
- 61.14.7. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado.

- 61.14.8. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados.
- 61.14.9. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 61.14.10. Possuir no mínimo 50 (cinquenta) categorias ou subcategorias de classificação de URL;
- 61.14.11. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 61.14.12. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 61.14.13. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários versus URL's, através da integração com serviços de diretório (LDAP/Active directory) e base de dados local;
- 61.14.14. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 61.14.15. Permitir a criação de categorias de URLs customizadas;
- 61.14.16. A solução deve forçar o acesso a sites de busca (Google, Bing e Yahoo), somente com a opção Safe Search habilitada;
- 61.14.17. Possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação/validação das URLs;
- 61.14.18. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
- 61.14.19. Permitir a customização de página de bloqueio;
- 61.14.20. Incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações, através da integração com serviços de diretório, via LDAP, Active directory, e base de dados local;
- 61.14.21. Possuir integração com LDAP, LDAP/AD para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on, essa funcionalidade não deve possuir limites licenciados de usuários ou não limitado a utilização de sistemas virtuais, segmentos de rede etc.;
- 61.14.22. Possuir integração com RADIUS e LDAP para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 61.14.23. Permitir o controle de acesso, para saída de Internet, sendo habilitado o captive portal, de forma integrada com a solução proposta;
- 61.14.24. Permitir e implementar o controle de acesso, habilitando o captive portal, baseados em

políticas definidas pela CONTRATANTE aderente;

- 61.14.25. Possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 61.14.26. Implementar a criação de grupos customizados de usuários no Firewall, baseado em atributos do LDAP e LDAP/AD;
- 61.14.27. Permitir a integração com tokens ou agentes para autenticação dos usuários;
- 61.14.28. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.
- 61.14.29. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual.
- 61.14.30. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra).
- 61.14.31. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido.
- 61.14.32. Deve filtrar o conteúdo baseado em categorias em tempo real.
- 61.14.33. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web.
- 61.14.34. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP.
- 61.14.35. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 61.14.36. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem.
- 61.14.37. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP.
- 61.14.38. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams.
- 61.14.39. Deve possuir Proxy Explícito e Transparente.
- 61.14.40. Deve implementar roteamento WCCP e ICAP.
- 61.15. FUNCIONALIDADE DE INTRUSION PREVENTION SYSTEM (IPS)
 - 61.15.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.
 - 61.15.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas.

- 61.15.3. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 61.15.4. Sincronizar entre membros de um cluster as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
- 61.15.5. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 61.15.6. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 61.15.7. Deve permitir funcionar em modo transparente, sniffer e router.
- 61.15.8. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.
- 61.15.9. Possuir, permitir, garantir, realizar e implementar os seguintes tipos de ações para ameaças detectadas pelo IPS ou Antivírus: permitir, permitir e gerar log, e bloquear;
- 61.15.10. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoração;
- 61.15.11. Possibilitar a criação de políticas por usuários, grupos de usuários, endereços IPs, redes ou zonas de segurança;
- 61.15.12. Possibilitar o uso de grupos de usuários da base LDAP, LDAP/AD do CONTRATANTE aderente, para aplicações de políticas baseadas nesses grupos;
- 61.15.13. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques, baseados em políticas do Firewall, considerando usuários, grupos de usuários, local ou base de usuários externas (LDAP, LDAP/AD);
- 61.15.14. Suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 61.15.15. Deve possuir capacidade de remontagem de pacotes para identificação de ataques.
- 61.15.16. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.
- 61.15.17. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.
- 61.15.18. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).

- 61.15.19. Deve possuir proteção contra-ataques DNS (Domain Name System).
- 61.15.20. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.
- 61.15.21. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).
- 61.15.22. Possuir os seguintes mecanismos de inspeção de IPS: Análise de padrões de estado de conexões, Análise de decodificação de protocolo; Análise para detecção de anomalias de protocolo; Análise heurística; Desfragmentação de IP; Remontagem de pacotes de TCP; Bloqueio de pacotes malformados;
- 61.15.23. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood etc.;
- 61.15.24. Detectar e bloquear a origem de programas de varredura de portas (portscans);
- 61.15.25. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 61.15.26. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 61.15.27. Permitir usar operadores de negação na criação de assinaturas ou políticas customizadas de IPS e anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 61.15.28. Permitir o bloqueio de vírus e Spywares em, pelo menos, três dos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 61.15.29. Identificar, alertar e bloquear comunicação com botnets;
- 61.15.30. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 61.15.31. Possuir, permitir, garantir, realizar, implementar e registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 61.15.32. Possuir, permitir, garantir, realizar, implementar e suportar a captura de pacotes (PCAP), em no mínimo um dos seguintes casos: por assinatura de IPS, ACL, controle de aplicação ou antimalware;
- 61.15.33. Permitir que na captura de pacotes por assinaturas de IPS ou ACL seja definido o número de pacotes a serem capturados, ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 61.15.34. Possuir a função de proteger resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

- 61.15.35. Identificar nos eventos o país de onde partiu a ameaça;
- 61.15.36. Incluir proteção contra vírus em conteúdo HTML e javascript, software espião (Spyware) e worms;
- 61.15.37. Ter proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- 61.15.38. Deve possuir alarmes na console de administração.
- 61.15.39. Deve possuir alertas via correio eletrônico.
- 61.15.40. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo Deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
- 61.15.41. Deve ter a capacidade de resposta/logs ativa a ataques.
- 61.15.42. Incluir proteção contra ataques de negação de serviços (DoS);
- 61.15.43. Possuir assinaturas específicas para a mitigação de ataques negação de serviços (DoS);
- 61.15.44. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;
- 61.16. FUNCIONALIDADE DE VPN
 - 61.16.1. Criar VPN dos tipos Site-to-Site e Client-To-Site;
 - 61.16.2. Suportar nativamente a criação de VPN IPSec utilizando 3DES;
 - 61.16.3. Suportar nativamente a criação de VPN IPSec utilizando AES (Advanced Encryption Standard) 128 ou 256 bits;
 - 61.16.4. Suportar nativamente a autenticação de VPN IPSec utilizando MD5 e SHA-1;
 - 61.16.5. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;
 - 61.16.6. Suportar nativamente a criação de VPN IPSec utilizando o algoritmo Internet Key Exchange (IKEv1 e v2);
 - 61.16.7. Suportar nativamente, para VPN IPSec, autenticação via certificado IKE PKI;
 - 61.16.8. Habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de resolução de problemas (troubleshooting);
 - 61.16.9. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais, como proxies;
 - 61.16.10. Realizar atribuição de DNS nos clientes remotos de VPN;

- 61.16.11. Permitir autenticação via AD/LDAP, certificados digitais, base de usuários local e soluções de autenticação multifator (MFA), incluindo tokens baseados em hardware ou software;
- 61.16.12. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 61.16.13. Permitir que a conexão com a VPN seja estabelecida antes ou após o usuário autenticar na estação;
- 61.16.14. Permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- 61.16.15. Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;
- 61.16.16. Possuir agente de VPN IPSEC client-to-site compatível com pelo menos: Windows, Linux e Mac OS.
- 61.16.17. Deve possuir hardware acelerador criptográfico para incrementar o desempenho de sessões e túneis IPsec estabelecidos.
- 61.17. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
 - 61.17.1. Reconhecer no mínimo 5.000 funções de aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, email, entre outros;
 - 61.17.2. Realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo, e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado, a aplicações usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado, o compartilhamento de arquivos;
 - 61.17.3. Atualizar a base de assinaturas de aplicações automaticamente;
 - 61.17.4. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações.
 - 61.17.5. Possibilitar adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
 - 61.17.6. Realizar múltiplos métodos de identificação e classificação das aplicações com, no mínimo, checagem de assinaturas e decodificação de protocolos;
 - 61.17.7. Realizar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do CONTRATANTE;

- 61.17.8. Permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 61.17.9. Permitir a configuração de alertas quando uma aplicação for bloqueada;
- 61.17.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 61.17.11. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos Peer-to-Peer (P2P) e permitir a aplicação de políticas de controle adequadas;
- 61.17.12. Possuir, permitir, garantir, realizar e implementar a diferenciação de tráfegos de mensageiros instantâneos, e permitir a aplicação de políticas de controle adequadas;
- 61.17.13. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 61.17.14. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como: P2P, Instant Messaging, Web client, Transferência de arquivos, VoIP.
- 61.17.15. A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.
- 61.17.16. Permitir a criação de grupos estáticos e dinâmicos de aplicações, definidos pela CONTRATANTE, baseados nas características das mesmas, tais como: tecnologia utilizada (Client-Server, BrowseBased, Network Protocol etc.), nível de risco, categoria, uso de técnicas evasivas, utilizadas por malwares (como uso excessivo de banda, tunelamento de tráfego ou transferência de arquivos), etc.
- 61.17.17. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 61.17.18. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 61.17.19. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados.
- 61.17.20. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory.
- 61.17.21. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory.

- 61.17.22. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP.
- 61.17.23. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem.
- 61.17.24. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino.
- 61.17.25. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.
- 61.17.26. Deve permitir criação de padrões de aplicação manualmente.
- 61.17.27. Deve permitir criar assinaturas personalizadas com o uso de expressões regulares e parâmetros de contexto, como sessões ou transações; sentido do fluxo, payload;
- 61.17.28. Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;
- 61.17.29. Possuir, permitir, garantir, realizar e implementar a diferenciação e controle de partes das aplicações como por exemplo permitir o chat e bloquear a chamada de vídeo;
- 61.17.30. Detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado, a Bittorrent "encriptado" e aplicações VOIP que utilizam criptografia proprietária;
- 61.18. FUNCIONALIDADE DE SD-WAN
 - 61.18.1. A solução de SD-WAN deve ser capaz de suportar tanto endereçamentos estáticos quanto dinâmicos, além de permitir a utilização simultânea de múltiplos links WAN de, de, no mínimo, 04 links de comunicação e transporte ativos.
 - 61.18.2. O plano de controle e orquestração SD-WAN deve ser local e operar de maneira autônoma no dispositivo, isto é, não serão aceitas soluções com plano de controle e orquestração SDWAN baseados em nuvem.
 - 61.18.3. A solução deve possuir, garantir, realizar, implementar o reconhecimento em camada 7 totalmente segregado da camada 4;
 - 61.18.4. A solução SD-WAN deve garantir, realizar, implementar e ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
 - 61.18.5. A solução SD-WAN deve possuir, garantir, realizar, implementar e suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
 - 61.18.6. A solução SD-WAN deve possuir, garantir, realizar, implementar e prover capacidade de inspeção SSL para a inspeção de tráfego https, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;
 - 61.18.7. A configuração VPN IPSEC deve possuir, garantir, implementar e oferecer suporte aos grupos DH (Diffie-Hellman) 14 e 15.

- 61.18.8. Deve possuir, garantir, realizar e implementar de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/range de IPs de destino;
- 61.18.9. A solução de SD-WAN deve possuir, garantir, realizar, implementar e suportar Roteamento dinâmico BGP com suporte a IPv6;
- 61.18.10. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 61.18.11. A solução deve possuir, garantir, implementar e permitir o estabelecimento automático de túneis VPN tipo Full-Mesh entre sites, sem necessidade de configuração explícita de túneis entre os mesmos.
- 61.18.12. A solução de SD-WAN deve possuir, garantir, implementar, permitir e suportar health check ativo, passivo e misto:
- 61.18.13. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
- 61.18.14. Passivo: uso do tráfego real para as medições;
- 61.18.15. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo.
- 61.18.16. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 61.18.17. A solução SD-WAN deve contar com recursos de segurança integrados, incluindo funcionalidades de firewall, VPN, antivírus, sistema de prevenção contra intrusões (IPS) e filtro de segurança web.
- 61.18.18. Deve possuir, garantir, realizar e implementar o reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
- 61.18.19. A solução deve possuir, garantir, realizar, implementar e ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter, Packet Loss e MOS (Mean Opinion Score), onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN, sem a obrigatoriedade de uma solução de gerenciamento externo;
- 61.18.20. Deve possuir, garantir, implementar e permitir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- 61.18.21. A solução SD-WAN deve oferecer inspeção SSL para análise do tráfego HTTPS, com o

objetivo de bloquear malwares e identificar aplicações em camada 7.

- 61.18.22. O reconhecimento de aplicações deve ocorrer de forma independente de porta ou protocolo, com inspeção direta do conteúdo dos pacotes (payload).
- 61.18.23. Deve possuir, garantir, realizar e implementar sobre o reconhecimento de Aplicações: a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook etc.);
- 61.18.24. Deverá possuir, garantir, implementar, permitir e ser capaz de prover Zero Touch provisioning, com capacidade de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;
- 61.18.25. A solução deve possuir, garantir, realizar, implementar e ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;
- 61.18.26. Deve possuir, garantir e implementar um mecanismo que permita definir um percentual mínimo de diferença entre os links medidos pelo SD-WAN, para que o chaveamento do tráfego para outro link ocorra automaticamente;
- 61.18.27. A solução deve possuir, garantir, implementar e permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
- 61.18.28. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- 61.18.29. Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;
- 61.19. IMPLANTAÇÃO, INTEGRAÇÃO E COMPATIBILIDADE
 - 61.19.1. A CONTRATADA será responsável por todas as etapas da implantação e configuração local, incluindo:
 - 61.19.1.1. Instalação e configuração da Solução de Segurança Cibernética NGFW, garantindo conectividade segura e controle de tráfego.
 - 61.19.1.2. Execução de testes operacionais e validação do funcionamento da solução antes da entrega formal à CONTRATANTE.
 - 61.19.2. Os componentes devem ser totalmente compatíveis e integrados com as soluções implantadas o Centro de Monitoramento e Controle, garantindo:

61.19.2.1. Gerenciamento centralizado por meio da Solução Centralizada de Monitoramento de Dispositivos.

61.19.2.2. Envio contínuo de logs para a Solução de Gerenciamento e Relatoria de Logs, permitindo análise de eventos e auditoria.

61.19.2.3. Padronização da infraestrutura de segurança e conectividade, facilitando a administração e monitoramento da rede.

62.LOTE - 02 - ITEM 37 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE SEGURANÇA DE REDE NGFW – TIPO 03

62.1.CARACTERÍSTICAS GERAIS:

62.1.1. Licenciamento e serviços de garantia técnica do Fabricante para o ITEM SOLUÇÃO DE SEGURANÇA DE REDE NGFW – TIPO III, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Otimização WAN.

62.1.2. Durante toda a vigência contratual em conjunto com serviços de garantia técnica oficial do fabricante a CONTRATADA deve prover serviços on-site através de sua própria equipe técnica. Isso inclui triagem inicial, verificação de configurações, coleta de logs (troubleshooting) e correções que não exijam alteração de código do software.

MATRIZ DE RISCOS
LOTE 01 – REDE GOVERNO V

Objeto de Aquisição:

Implantação de Sistema de Registro de Preços para contratação de empresa especializada em Tecnologia da Informação e Comunicação (TIC), visando ao fornecimento de solução corporativa integrada de conectividade segura para a Rede Governo V, abrangendo serviços de conectividade de dados, segurança da informação, monitoramento, gestão centralizada, manutenção e suporte continuado.

Identificação dos Riscos				
Código do Risco	Descrição do Risco	Consequências	Data (Identificação)	Quem Identificou o Risco
1	Atraso na transição do modelo vigente da Rede Governo IV para a Rede Governo V	Risco de descontinuidade parcial dos serviços de conectividade e impacto sobre a prestação de serviços públicos essenciais	Planejamento da contratação	Equipe de planejamento
2	Instabilidade econômico-financeira da empresa contratada ao longo da vigência da Ata	Comprometimento da capacidade de execução continuada dos serviços e risco à continuidade da Rede Governo	Planejamento da contratação	Equipe de planejamento
3	Falhas na integração da solução contratada aos mecanismos corporativos de gestão e monitoramento da Rede Governo	Redução da efetividade da governança centralizada, dificuldades de fiscalização e aumento do risco operacional	Planejamento da contratação	Equipe de planejamento
4	Indisponibilidade ou degradação de desempenho da conectividade durante a execução contratual	Impacto direto sobre sistemas corporativos, serviços digitais e atividades finalísticas dos órgãos e entidades	Planejamento da contratação	Equipe de planejamento
5	Divergências quanto à demanda efetiva dos órgãos aderentes à Ata de Registro de Preços	Risco de subutilização ou insuficiência da solução contratada, com impacto econômico e operacional	Planejamento da contratação	Equipe de planejamento
6	Falhas na fiscalização e no acompanhamento da execução contratual	Execução inadequada dos serviços, dificuldade de apuração de responsabilidades e risco jurídico	Planejamento da contratação	Equipe de planejamento
7	Descumprimento de	Risco jurídico,	Planejamento	Equipe de

Avaliação dos Riscos Probabilidade x Impacto			
Probabilidade da Ocorrência	Impacto do Risco	Nível do Risco	
		Valor	Classificação
Média	Grande	12,00	Alto
Baixa	Grande	8,00	Médio
Média	Moderado	9,00	Médio
Média	Grande	12,00	Alto
Média	Moderado	9,00	Médio
Baixa	Moderado	6,00	Médio
Baixa	Grande	8,00	Médio

Planejamento de Resposta aos Riscos			
Estratégia de Resposta	Ações/Resposta	Item de Mitigação no TR	Responsabilidade
Reduzir	Definição de cronograma de transição gradual, com coexistência controlada dos ambientes até a plena estabilização da nova rede	Modelo de implantação e cronograma de transição da solução	Compartilhada
Reduzir	Exigência de comprovação de qualificação econômico-financeira compatível com a complexidade e o vulto da contratação	Habilitação econômico-financeira	Contratante
Reduzir	Definição de requisitos técnicos mínimos de interoperabilidade, integração e compatibilidade com os sistemas corporativos existentes	Requisitos técnicos da solução e integração com sistemas corporativos	Contratada
Reduzir	Estabelecimento de níveis mínimos de serviço, indicadores de desempenho e penalidades por descumprimento	Níveis de Serviço (SLA) e sanções contratuais	Contratada
Reduzir	Adoção do Sistema de Registro de Preços, permitindo flexibilidade controlada de contratação conforme a necessidade real	Regras de utilização da Ata de Registro de Preços	Compartilhada
Reduzir	Definição clara do modelo de gestão e fiscalização do contrato, com responsabilidades e procedimentos formalizados	Modelo de gestão e fiscalização contratual	Contratante
Reduzir	Vinculação expressa da	Obrigações legais e	Contratada

	requisitos legais e normativos aplicáveis à governança da Rede Governo	necessidade de ajustes contratuais e impacto na continuidade do serviço	da contratação	planejamento
8	Dependência excessiva de fornecedores ou tecnologias específicas	Restrição à competitividade futura, dificuldades de substituição e risco à continuidade da Rede Governo	Planejamento da contratação	Equipe de planejamento

Baixa	Moderado	6,00	Médio

	execução contratual às diretrizes legais, normativas e institucionais aplicáveis	normativas da contratada	
Reduzir	Definição de requisitos técnicos baseados em desempenho e interoperabilidade, evitando amarras indevidas	Requisitos técnicos e critérios de aceitabilidade	Contratante

MATRIZ DE RISCOS

LOTE 02 – SOLUÇÕES DE SEGURANÇA

Objeto de Aquisição:

Implantação de Sistema de Registro de Preços para contratação de empresa especializada em Tecnologia da Informação e Comunicação (TIC), visando ao fornecimento, licenciamento, atualização de funcionalidades, implantação, suporte, garantia e operação continuada de soluções corporativas de segurança da informação, abrangendo, entre outras, firewalls de próxima geração, soluções de proteção de endpoints, correlação e relatoria de eventos, autenticação, monitoramento e gestão centralizada de segurança.

Identificação dos Riscos					Avaliação dos Riscos Probabilidade x Impacto				Planejamento de Resposta aos Riscos			
Código do Risco	Descrição do Risco	Consequências	Data (Identificação)	Quem Identificou o Risco	Probabilidade da Ocorrência	Impacto do Risco	Nível do Risco		Estratégia de Resposta	Ações/Resposta	Item de Mitigação no TR	Responsabilidade
							Valor	Classificação				
1	Descontinuidade do licenciamento ou das atualizações das soluções de segurança durante a vigência da Ata	Obsolescência tecnológica, perda de efetividade dos mecanismos de proteção, aumento da exposição a ameaças cibernéticas e comprometimento da continuidade dos serviços públicos digitais	Planejamento da contratação	Equipe de planejamento	Média	Grande	12,00	Alto	Reduzir	Definição de escopo contratual que contemple licenciamento ativo e atualizações contínuas durante toda a vigência	Escopo do licenciamento e atualização das soluções	Contratada
2	Falhas na integração das soluções contratadas com a infraestrutura corporativa de segurança existente	Redução da visibilidade, dificuldade de correlação de eventos, fragilização da governança centralizada e aumento do risco operacional	Planejamento da contratação	Equipe de planejamento	Média	Moderado	9,00	Médio	Reduzir	Estabelecimento de requisitos técnicos mínimos de compatibilidade, interoperabilidade e integração com soluções corporativas existentes	Requisitos técnicos e de integração das soluções	Contratada
3	Incapacidade técnica da contratada para operar e sustentar soluções de segurança de missão crítica	Falhas recorrentes, baixa qualidade dos serviços, aumento de incidentes de segurança e risco à continuidade operacional	Planejamento da contratação	Equipe de planejamento	Baixa	Grande	8,00	Médio	Reduzir	Exigência de comprovação de qualificação técnica compatível com a complexidade do objeto	Qualificação técnica	Contratante
4	Descumprimento dos níveis mínimos de serviço estabelecidos para suporte, atendimento e operação	Atrasos na resolução de incidentes, indisponibilidade prolongada das soluções e impacto sobre serviços críticos	Planejamento da contratação	Equipe de planejamento	Média	Grande	12,00	Alto	Reduzir	Definição de SLAs objetivos, métricas de desempenho e penalidades proporcionais ao descumprimento	Níveis de Serviço (SLA) e sanções contratuais	Contratada
5	Tratamento inadequado de dados pessoais no contexto da operação das	Exposição de dados sensíveis, responsabilização administrativa e jurídica	Planejamento da contratação	Equipe de planejamento	Baixa	Grande	8,00	Médio	Reduzir	Inclusão de cláusulas específicas de observância integral à legislação de proteção de dados pessoais	Proteção de Dados Pessoais	Contratada

	soluções de segurança	da Administração		
6	Divergências quanto à demanda efetiva dos órgãos aderentes à Ata de Registro de Preços	Risco de subutilização ou insuficiência de licenças e serviços, com impacto econômico e operacional	Planejamento da contratação	Equipe de planejamento
7	Falhas na fiscalização e no acompanhamento da execução dos serviços gerenciados de segurança	Dificuldade de comprovação de entregas, baixa efetividade da gestão contratual e risco jurídico	Planejamento da contratação	Equipe de planejamento
8	Dependência excessiva de fornecedores ou tecnologias específicas	Restrição à competitividade futura, dificuldades de substituição e risco à continuidade da Rede Governo	Planejamento da contratação	Equipe de planejamento

Média	Moderado	9,00	Médio
Baixa	Moderado	6,00	Médio
Baixa	Moderado	6,00	Médio

Reduzir	Adoção do Sistema de Registro de Preços, assegurando flexibilidade controlada de contratação conforme a necessidade real	Regras de utilização da Ata de Registro de Preços	Compartilhada
Reduzir	Definição de modelo formal de gestão, fiscalização, registro de ocorrências e validação de entregas	Modelo de gestão e fiscalização contratual	Contratante
Reduzir	Definição de requisitos técnicos baseados em desempenho e interoperabilidade, evitando amarras indevidas	Requisitos técnicos e critérios de aceitabilidade	Contratante