Cia. de Processamento de Dados do Estado da Bahia
Avenida 4, nº 410, Centro Administrativo da Bahia – CAB
Tel. (71) 3115-7611 Fax (71) 3371-5787 CEP 41.745-002
CNPJ 13.579.586/0001-32 Insc. Estadual 70.695.593
Caixa Postal 678 Salvador - Bahia - Brasil
www.prodeb.ba.gov.br

PRODEB
TECNOLOGIA, INFORMAÇÃO E SEGURANÇA.

CONTRATO Nº 24/136-01 – PRESTAÇÃO DE SERVIÇOS

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 o **CONSÓRCIO CYBERSEC BAHIA,** inscrito no CNPJ nº 55.904.689/0001-70, formado pelas empresas TLD HUB DE CIBERSEGURANÇA & CONECTIVIDADE LTDA, CNPJ nº 33.927.849/0001-64 e CENTRO DE PESQUISAS EM INFORMÁTICA LTDA, CNPJ nº 40.584.096/0001-05, com sede na Rua Soldado Luiz Gonzaga das Virgens, 111, Edf. Liz Corporate, andar 4, Caminho das Árvores, Salvador/BA, CEP 41.820-560, legalmente representada pelos Srs. Ricardo Luiz de Oliveira, portador da cédula de identidade nº 07.352.838-26, emitida por SSP/BA, inscrito no CPF/MF sob o nº 684.548.135-00 e João Gualberto Rizzo Araújo, portador da cédula de identidade nº 3.688.884-28, emitida por SSP/BA, inscrito no CPF/MF sob o nº 506.901.245-20, doravante denominada simplesmente **CONTRATADA** com respaldo no rito similar ao Pregão Eletrônico nº 006/2024 de que trata o Processo Administrativo SEI nº 065.10933.2023.0013168-58 e 065.10933.2024.0010814-61, 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, e subsidiariamente, pelas Leis nºs 8.666/93, 9.433/2005, na forma autorizada pelo Diretor Executivo da Prodeb (doc. SEI nº 00081794631), 10.520/2002, bem como pela Lei Complementar nº 123/2006 e suas alterações, dos Decretos Estaduais nº 18.471 de 29 de junho de 2018 e nº 19.896 de 05 de agosto de 2020 e demais legislações pertinentes, mediante as cláusulas e condições a seguir ajustadas:

CLÁUSULA PRIMEIRA – FUNDAMENTO LEGAL

O presente ajuste – na forma do Regulamento de Licitações e Contratos – RLC da PRODEB, aprovado pelo CAD em 29/06/2018, decorre do Pregão Eletrônico nº 006/2024, devidamente homologado em 21/06/2024 pela Diretoria Executiva da CONTRATANTE (DOC. SEI nº 00092609524), tudo constante dos Processos Administrativos SEI nº 065.10933.2023.0013168-58 e 065.10933.2024.0010814-61, que fica fazendo parte integrante do presente contrato, regendo-o no que for omisso.

CLÁUSULA SEGUNDA - OBJETO

Constitui objeto do presente instrumento a contratação de empresa especializada em Tecnologia da Informação e Comunicação (TIC) para fornecimento de soluções de segurança incluindo Next-Generation Firewalls (NGFW), soluções para Endpoints, Email, Autenticação de Múltiplos Fatores (MFA) e Honeypot contemplando serviços de implantação, suporte, garantia e serviços continuados gerenciados de segurança da informação, além da prestação de serviços gerenciados continuados englobando operação, atendimento de requisições, gestão de incidentes e vulnerabilidades e monitoramento das soluções de segurança já existentes implantadas no datacenter PRODEB, de acordo com as especificações e obrigações consignadas na Requisição de Compras nº 026913, no Termo de Referência que constitui o ANEXO I, 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 00087288361), parte integrante deste Contrato**.**

§2º É vedada a subcontratação parcial 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 na alínea "f", da Cláusula Décima Sexta deste instrumento.

§3º Os serviços objeto deste contrato não podem sofrer solução de continuidade durante todo o prazo da sua vigência, devendo ser executados por empregados/prepostos da CONTRATADA, sob a inteira responsabilidade funcional e

operacional desta, mediante vínculo de subordinação dos trabalhadores para com a empresa contratada, sobre os quais manterá estrito e exclusivo controle.

CLÁUSULA TERCEIRA - PRAZO

O prazo de vigência do contrato a contar da data da sua assinatura, será de 28 (vinte e oito) meses, ficando a sua eficácia condicionada à publicação do extrato na imprensa oficial, admitindo-se a sua prorrogação, para os itens 1 e 2 e os serviços dos itens 09 à 13, nos termos e condições dos artigos 71 e 81 da Lei n° 13.303/2016, com correspondência nos artigos 164 do RLC/PRODEB, e demais normas concernentes à matéria, **conforme previsto no item 20 do Termo de Referência.**

§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. 187, Parágrafo único do Regulamento de Licitações e Contratos - RLC da PRODEB.

§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 descritos na **CLÁUSULA SEGUNDA** do presente instrumento, os valores devidos de acordo com o previsto no item 18 do Termo de Referência, possuindo o presente contrato o valor global de **R$ 9.120.000,00 (nove milhões cento e vinte mil reais)**, conforme proposta da CONTRATADA datada de 06/11/2024, acostada ao Processo Administrativo SEI n° 065.10933.2024.0010814-61, ora passando a integrar o ANEXO II deste instrumento.

ITEM	DESCRITIVO	QUANTIDADE	VALOR MENSAL	VALOR TOTAL (24 meses)
09	Serviços Profissionais de Monitoramento e Segurança do Datacenter da PRODEB pelo período de 24 Meses.	01	R$ 380.000,00	R$ 9.120.000,00

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 § 4° do art. 81 da Lei n° 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
COSUR	RECURSOS PRÓPRIOS	4111050101 TEC-LICENÇA DE USO DE SOFTWARE

CLÁUSULA SEXTA - PAGAMENTO

Em consonância com o **§1º do art. 207** 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:

a) até R$ 50.000,00 o pagamento será efetuado em até 15 (quinze) dias;

b) de R$ 50.000,01 a R$ 100.000,00 o pagamento será efetuado em até 30 (trinta) dias;

c) 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:

a) prova de regularidade relativa à Seguridade Social (INSS) e ao Fundo de Garantia por Tempo de Serviço (FGTS);

b) 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.

c) prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação da Certidão Negativa de Débitos Trabalhistas (CNDT);

d) certidão de regularidade com a Fazenda Pública Municipal (referente ao INSS) 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 Fiscaldo 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 § 7°, da Cláusula Décima Terceira deste instrumento.

§4º A(s) nota(s) fisca(l)is/fatura(s) deverá(ao) 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 vigo.

§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 § 1° do artigo 162, 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. 162, 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. 163, incisos I, II e III, §§ 1° e 2° 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. 180 do Regulamento de Licitações e Contratos – RLC da PRODEB.

§1º A revisão de preços, nos termos do art. 182 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.

§5° 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 no **item 22.1 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.

CLÁUSULA DÉCIMA - OBRIGAÇÕES DA CONTRATANTE

A **CONTRATANTE,** além das obrigações contidas neste contrato por determinação legal e no **item 22.2 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 global.

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.

§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 190 a 206 do Regulamento de Licitações e Contratos – RLC da PRODEB, 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, conforme o artigo 191, inc. XII, do Regulamento de Licitações e Contratos – RLC da PRODEB.

§3º O recebimento do objeto se dará segundo o disposto nos artigos 201 a 205 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 Antônio Carlos Andrade Borges Junior - Gerência de Tecnologia e Conectividade (GTC), matrícula nº 92060794 e como Fiscal Sr. Fabricio de Souza Pinto, Coordenador de Suporte a Rede, Matrícula nº 65002945.

§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 211, inc. II, do Regulamento de Licitações e Contratos – RLC da PRODEB, observados os parâmetros estabelecidos nesta cláusula, sem prejuízo da rescisão unilateral do contrato (artigo 209 do Regulamento de Licitações e Contratos – RLC da PRODEB), a qualquer tempo, e a aplicação das demais sanções previstas no citado RLC, bem como na Lei estadual nº 9.433/05.

§1º Em caso de descumprimento total da obrigação principal, será aplicada multa no percentual 10% (dez por cento) incidente sobre o valor global do contrato.

§2º Caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicado o percentual 10% (dez por cento) sobre o saldo do contrato, isto é, sobre a diferença entre o valor global do contrato e o valor da parte do fornecimento, da obra ou do serviço já realizado.

§3º Em caso de atraso no cumprimento da obrigação principal, será aplicado o percentual de 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, e de 0,7% (sete décimos por cento) por cada dia subsequente ao trigésimo, calculados sobre o valor da parcela do fornecimento, da obra ou do serviço em mora.

§4º Na hipótese do parágrafo anterior, se a multa moratória atingir o patamar de 10% (dez por cento) do valor global do contrato, deverá, salvo justificativa escrita devidamente fundamentada, ser recusado o recebimento do objeto, sem prejuízo da aplicação das demais sanções previstas no RLC e na lei.

§5º Na hipótese de a CONTRATADA se negar a efetuar o reforço da garantia, dentro de 10 (dez) dias contados da data de sua convocação, será aplicada multa no percentual de 2,5% (dois e meio por cento) incidente sobre o valor global do contrato.

§6º 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.

§7º 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 207, § 11, do Regulamento de Licitações e Contratos – RLC da PRODEB.

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 VI e VII do art. 184 e I, IV, VI e VII do art. 185 da Lei estadual nº 9.433/05.

§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.

§2º A reincidência da sanção de advertência poderá ensejar a aplicação da penalidade de suspensão do direito de licitar e impedimento de contratar com a CONTRATANTE ou aplicação de multa no valor de 5% (cinco por cento) do valor do contrato, conforme o caso.

§3º Para a aplicação das penalidades previstas serão levados em conta a natureza e a gravidade da falta, os prejuízos dela advindos para a CONTRATANTE e a reincidência na prática do ato.

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 n° 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 (dezesseis) 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 209, §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 208 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 III 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 IV – 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 INSTUMENTO 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 - TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE
ANEXO V – 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 dirimir quaisquer dúvidas oriundas do presente contrato, renunciando a qualquer outro por mais privilegiado que seja.

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

Salvador, ____ de _____ de 2024.

Pela **CONTRATANTE/PRODEB**:

_____

José Muniz Rebouças
Diretor Executivo

_____

Carlos Augusto Borges Silva

Diretor de Infraestrutura Tecnológica e Conectividade

Pela **CONTRATADA:**

_____

Consórcio Cybersec Bahia

ANEXO I – TERMO DE REFERÊNCIA

Termo de Referência (TR)

Contratação de Serviços Gerenciados e Soluções de Segurança

PRODEB

TECNOLOGIA, INFORMAÇÃO E SEGURANÇA.

TERMO DE REFERÊNCIA – CONTRATAÇÃO DE SERVIÇOS GERENCIADOS E SOLUÇÕES DE SEGURANÇA

I. DA CONTRATAÇÃO

1. OBJETO DA CONTRATAÇÃO

1.1. Implantação de Sistema de Registro de Preços objetivando a formalização de ata com o vencedor do certame, visando à contratação de empresa especializada em Tecnologia da Informação e Comunicação (TIC) para fornecimento de soluções de segurança incluindo Next-Generation Firewalls (NGFW), soluções para Endpoints, Email, Autenticação de Múltiplos Fatores (MFA) e Honeypot contemplando serviços de implantação, suporte, garantia e serviços continuados gerenciados de segurança da informação, além da prestação de serviços gerenciados continuados englobando operação, atendimento de requisições, gestão de incidentes e vulnerabilidades e monitoramento das soluções de segurança já existentes implantadas no datacenter PRODEB.

1.2. Considerando que o objeto que se pretende contratar pode ser descrito de forma objetiva, como consta neste termo de referência, bem como, que a técnica para sua realização é perfeitamente conhecida, dominada e oferecida pelo mercado, o mesmo pode ser enquadrado como de natureza comum;

1.3. O serviço a ser contratado será gerenciado tecnicamente pela COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DA BAHIA (PRODEB), estando as partes interessadas na referida contratação relacionadas abaixo:

PARTICIPANTES: poderão contratar os itens constantes deste registro de preços a PRODEB e os Órgãos e Entidades da Administração Pública do Estado da Bahia.

GESTOR TÉCNICO DA SOLUÇÃO: PRODEB.

FORNECEDOR BENEFICIÁRIO DO REGISTRO DE PREÇO: Empresa vencedora do certame.

1.4. Os itens 06, 07, 08 e 09 serão consumidos exclusivamente pela Prodeb devido a terem sido planejados para atender especificamente a infraestrutura de segurança instalada em seu Data Center e a capacidade para atender a todo o Governo do Estado.

II. JUSTIFICATIVA DA CONTRATAÇÃO

A Companhia de Processamento de Dados do Estado da Bahia - PRODEB, sociedade de economia mista, integrante do Poder Executivo do Estado da Bahia, tem a finalidade de prover serviços de Tecnologia da Informação e Comunicação – TIC com segurança, confiabilidade e disponibilidade, garantindo a continuidade dos negócios e a proteção das informações dos Órgãos e Entidades do Estado da Bahia.

Diante do constante avanço tecnológico e da crescente oferta de serviços digitais à população, o Governo do Estado, por meio da PRODEB, tem direcionado investimentos significativos na área de Segurança da Informação. A disponibilização de novas plataformas digitais tem trazido inúmeras facilidades aos cidadãos, no entanto, esse cenário também acompanha uma preocupação com a proteção dos usuários e dados, devido ao aumento proporcional da exposição e do risco de ataques cibernéticos, representando uma ameaça à integridade dos dados sensíveis dos cidadãos e à continuidade dos serviços públicos.

Nesse contexto, a PRODEB tem adotado uma abordagem contundente e proativa, buscando implementar medidas de segurança avançadas e robustas para proteger a infraestrutura tecnológica do Estado e garantir a segurança das informações. Isso inclui a utilização de tecnologias de ponta, a realização de auditorias de segurança regulares, a implementação de políticas e controle de acesso, além do constante aprimoramento das práticas de segurança cibernética, visando mitigar os riscos, preservar o sigilo, a integridade e a disponibilidade das informações.

Essas soluções de segurança, gerenciadas pela PRODEB, concentram-se na proteção das camadas de Internet e Datacenter. No entanto, há uma infraestrutura corporativa complexa que interliga todas as unidades dos Órgãos do Governo do Estado da Bahia em uma extensa rede privada de comunicação de dados. Essa rede é composta pela Rede Governo III e IV e IDB

(Infovia Digital da Bahia) que funcionam de forma integrada e permite que as unidades se comuniquem entre si, facilitando o acesso aos serviços e otimizando os processos operacionais. A PRODEB atua como gestora técnica dessas Redes atuando na manutenção, suporte, monitoramento e gerenciamento das mesmas, mas sem ultrapassar o limite da Rede Local das unidades, pois são de responsabilidade de cada Órgão e Entidade.

Com o intuito de aumentar a segurança e a visibilidade do tráfego de dados transmitidos diariamente nestas redes corporativas privadas, foi adquirida em 2023 a solução de Network Detection and Responde (NDR). Esta solução tem realizado a detecção de tráfegos maliciosos não só em direção ao Datacenter da PRODEB, mas também movimentações laterais entre unidades que utilizam essa rede. São identificados cerca de 3,4 milhões de eventos e realizados mais de 1 milhão de bloqueios mensalmente.

Essa contenção é realizada nos dispositivos de segurança administrados pela PRODEB que estão localizados nas camadas do Datacenter e da Internet, evitando a proliferação dessas ameaças e protegendo os servidores hospedados no Data Center da Companhia, mas devido a grande parte desse tráfego ser originado por equipamentos localizados nas Redes Locais (LAN´s) das sedes ou unidades remotas dos Órgãos, **onde a PRODEB não realiza qualquer gestão**, são enviadas notificações às equipes de Tecnologia locais dessas Entidades para tratamento, contenção e erradicação da ameaça dos equipamentos comprometidos, que por muitas vezes, não conseguem realizar de forma célere e efetiva.

Visto que os Órgãos da Administração Pública têm como objetivo principal a prestação de serviços ao cidadão, e para isso, precisam concentrar seus esforços em suas atividades fim, que são aquelas que estão diretamente relacionadas à sua missão. Sendo assim, para aprimorar a proteção em um nível de maior granularidade, trazendo segurança para os diversos dispositivos conectados, para minimizar o **risco de vazamento** e comprometimento de dados sensíveis e o **risco de indisponibilidade** de serviços essenciais por tempo indeterminado, torna-se de fundamental importância a **aquisição de soluções de segurança com foco na proteção das Redes Locais dos Órgãos do Governo do Estado**, juntamente com contratação de serviço de monitoramento, gerenciamento e contenção contra ataques cibernéticos para atuação contínua e ininterrupta. Esse serviço de gerenciamento deve abranger também as soluções de segurança instalados no Datacenter da Prodeb, garantindo integração e continuidade da operação de cibersegurança em todo Governo do Estado.

Ademais, vale ressaltar, que a utilização do sistema de registro de preços se justifica, uma vez que a implantação desse ferramental ocorrerá de forma paulatina, ajustada de acordo com as especificidades de cada órgão/cliente, de modo que as contratações serão efetivadas à medida que a PRODEB venha sendo demanda.

III. DO DETALHAMENTO DA SOLUÇÃO

2. DETALHAMENTO DO OBJETO – LOTE ÚNICO

ITENS DE SOFTWARE E HARDWARE			
ITEM	**DESCRITIVO**	**UNID**	**QUANTIDADE**
01	Solução de Segurança de Endpoint - EPP	UN	2500
02	Solução para duplo Fator de Autenticação - Token Mobile	UN	750
03	Solução de Segurança de Rede NGFW TIPO I	UN	450
04	Solução de Segurança de Rede NGFW TIPO II	UN	60
05	Solução de Segurança de Aplicações WAF TIPO I	UN	08
06	Solução de Segurança de Aplicações WAF TIPO II	UN	02
07	Solução de Segurança Decoy/Honeypot	UN	04
08	Solução de Segurança de Email.	UN	02

ITENS DE SERVIÇOS			
ITEM	**DESCRITIVO**	**UNID**	**QUANTIDADE**

09	Serviços Profissionais de Monitoramento e Segurança do Datacenter da PRODEB pelo período de 24 Meses.	UN	1
10	Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Endpoint - EPP" para cada item monitorado pelo período de 24 Meses.	UN	62.500
11	Serviços Profissionais de Monitoramento e Segurança para o item "Solução para duplo Fator de Autenticação - Token Mobile" para cada item monitorado pelo período de 24 Meses.	UN	3.750
12	Serviços Profissionais de Monitoramento e Segurança para os itens "Solução de Segurança de Rede NGFW TIPO I, II" para cada item monitorado pelo período de 24 Meses.	UN	510
13	Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Aplicações WAF TIPO I" para cada item monitorado pelo período de 24 Meses.	UN	08

3. DETALHAMENTO DAS ESPECIFICAÇÕES TÉCNICAS

3.1. ITEM 01 – SOLUÇÃO DE SEGURANÇA DE ENDPOINT – EPP

3.1.1. Deve permitir a instalação, gerência e atualizações das funcionalidades de 25 (vinte e cinco) endpoints, durante toda vigência contratual 24 (vinte e quatro) meses;
3.1.2. Deve permitir o gerenciamento dos clientes de segurança remotamente, a partir de um console central do próprio fabricante;
3.1.3. Deve possui funcionalidade Zero Trust Applied, com túneis criptografados automáticos para controle acesso validado por sessão a aplicativos, através de funcionalidade de avaliação de postura do EndPoint;
3.1.4. Deve estar licenciados com as funcionalidades de AI Powered NGAV, Cloud Sandbox, Automated Endpoint Quarantine, Application Firewall e Application Inventory;
3.1.5. O licenciamento deve se basear no número de clientes registrados no console de gerenciamento central do mesmo fabricante;
3.1.6. Deve ser fornecida Solução Centralizada de Armazenamento de Logs e Relatórios, caso compatível poderá ser utilizada atual solução existente na PRODEB, Marca Fortinet, Modelo FAZ-3700G;
3.1.7. Deve ser compatível e permitir integração com atual "SOLUÇÃO AUTENTICAÇÃO E GERENCIAMENTO DE ACESSO" existente na PRODEB, e com itens "SOLUÇAO DE SEGURANÇA DE REDE NGFW TIPO I, II"
3.1.8. Deve ser compatível com pelos menos os seguintes sistemas operacionais:
  3.1.8.1. Microsoft Windows: 7 (32 e 64 bits), 8 (32 e 64 bits), 8,1 (32 e 64 bits), 10 (32 e 64 bits) e 11 (64 bits);
  3.1.8.2. Microsoft Windows Server: 2012, 2012 R2, 2016 e 2019;
  3.1.8.3. Mac OS 11+, v10.14, v10.15;
  3.1.8.4. Android 5.0 e superiores;
  3.1.8.5. Linux Ubuntu 16.04, CentOs 7.4;
3.1.9. Deve ter uma interface gráfica do usuário, pelo menos nos idiomas inglês, português e espanhol;
3.1.10. Deve permitir o backup do arquivo de configuração;
3.1.11. Deve ser capaz de gerar um diário (logs) nas funcionalidades instaladas e configuradas;
3.1.12. Deve suportar pelo menos os seguintes níveis de log devem estar disponíveis: emergência, alerta, crítico, erro, aviso, informativo;
3.1.13. Os clientes de segurança deverão poder enviar os logs para o servidor console de gerenciamento central;
3.1.14. Os clientes de segurança deverão permitir a configuração local via XML (eXtensible Markup Language);
3.1.15. Os clientes de segurança deverão suportar integração às tecnologias Sandboxing pelo menos do mesmo fabricante;
3.1.16. Deve controlar o acesso a dispositivos removíveis e ser capaz de monitorar, permitir ou negar acesso a dispositivos USB
3.1.17. Deve poder definir o nível do log: emergência, alerta, crítico, erro, aviso, aviso, depuração, informações;
3.1.18. Deve ter um agente de logon único;
3.1.19. Deve ter a capacidade de desabilitar os serviços de proxy para erros de depuração;
3.1.20. Deve ser capaz de ativar seletivamente logs em: VPN, Antivírus, Atualizações, Sandboxing, Comunicação com segurança cooperativa, filtro de web e verificação de vulnerabilidade;
3.1.21. Deve suportar exportar os logs para fora do cliente de segurança
3.1.22. FUNCIONALIDADES DE ANÁLISE COOPERATIVA

3.1.22.1. Deve ser capaz de integrar a uma estrutura cooperativa para compartilhar informações e receber atualizações de assinaturas dinâmicas;
3.1.22.2. Deve suportar o envio de logs para um analisador central de logs, onde os índices de compromissos do cliente (IoC) seja processado (taxas de confirmação)
3.1.22.3. Deve suportar receber atualizações de assinaturas dinâmicas da solução de proteção avançada de ameaças (ATP) ou sandboxing
3.1.22.4. Deve ser disponibilizado uma ferramenta que permita a aplicação de políticas diferentes, independente do cliente estar conectado ou não à rede corporativa;
3.1.22.5. Deve permitir ficar em quarentena no console central ou em algum outro componente que faça parte da solução de segurança cooperativa.

3.1.23. FUNCIONALIDADES DE ANTIVÍRUS
3.1.23.1. O cliente de segurança deve ter a capacidade de inspecionar arquivos executáveis, bibliotecas e drivers quanto a vírus;
3.1.23.2. O cliente de segurança deve ser capaz de verificar atualizações de assinatura automaticamente
3.1.23.3. O cliente de segurança deve ser capaz de enviar arquivos para inspeção nos sistemas Sandboxing do mesmo fabricante;
3.1.23.4. O cliente de segurança deve ser capaz de bloquear os canais de comunicação usados por hackers ou atacantes;
3.1.23.5. O cliente de segurança deve notificar localmente quando um vírus é detectado
3.1.23.6. O cliente de segurança deve permitir que o usuário inicie uma verificação sob demanda
3.1.23.7. O cliente de segurança deve permitir que a verificação de vírus seja iniciada automaticamente regularmente
3.1.23.8. O cliente de segurança deve permitir a visualização dos arquivos em quarentena
3.1.23.9. Deve permitir a configuração do perfil antivírus a partir do console central do mesmo fabricante
3.1.23.10. Deve 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.
3.1.23.11. A ferramenta de proteção baseada em nuvem NÃO deve enviar o arquivo inteiro ou seus metadados. SOMENTE a soma de verificação
3.1.23.12. A ferramenta de proteção baseada em nuvem deve analisar apenas arquivos de alto risco, como, entre outros, documentos do Word, Excel, PDF e DLL.
3.1.23.13. Deve ter uma solução de Anti-Exploit, que protege o endpoint de ameaças em tempo real, observando o comportamento de aplicativos populares, incluindo os leitores do Office, Internet Explorer, Chrome, Firefox, Java, Java, Flash e PDF. Etc
3.1.23.14. Deve ser capaz de enviar arquivos para uma solução de proteção avançada de ameaças (ATP) (ou sandboxing) antes de ser acessado;
3.1.23.15. Deve suportar sandbox localmente ou através de uma solução em nuvem
3.1.23.16. Deve ser capaz de bloquear o acesso ao arquivo até que o sandbox dê um veredicto
3.1.23.17. Caso um arquivo seja marcado como malicioso pela Sandbox, o mesmo deve ser mantido em quarentena;

3.1.24. FUNCIONALIDADES DE FIREWALL DE APLICATIVOS
3.1.24.1. O cliente de segurança deve suportar perfis de Controle de Aplicativos, criados centralmente no console de gerenciamento do mesmo fabricante;
3.1.24.2. O fabricante deve permitir que os clientes de segurança façam consultas on-line sobre a categoria de um determinado aplicativo a ser usado na política de controle de acesso
3.1.24.3. Deve possuir pelo menos 4000 aplicativos reconhecidos em sua base para que possam ser usados nas regras de controle de acesso dos clientes de segurança

3.1.25. FUNCIONALIDADES DE VPN IPSEC
3.1.25.1. Deve permitir que o usuário crie novas VPNs IPSEC
3.1.25.2. Deve permitir que várias VPNs IPSEC sejam definidas simultaneamente
3.1.25.3. Deve permitir a autenticação usando nome de usuário e senha
3.1.25.4. Deve permitir a autenticação usando certificados digitais
3.1.25.5. Deve permitir a seleção dos modos Principal e Agressivo;
3.1.25.6. Deve permitir a configuração do DHCP por IPSec;
3.1.25.7. Deve permitir o uso do NAT Traversal;
3.1.25.8. Deve permitir a escolha de grupos Diffie-Hellman (1,2,5 e 14);
3.1.25.9. Deve permitir configurações de expiração de chave IKE;
3.1.25.10. Deve suportar IKEv1 e IKEv2

3.1.25.11. Deve permitir o uso do Perfect Forward Secrecy;
3.1.25.12. Deve permitir a autenticação de dois fatores fornecida pelo mesmo fabricante

3.1.26. FUNCIONALIDADES DE VPN SSL

3.1.26.1. Deve permitir que o usuário crie novas VPNs SSL
3.1.26.2. Deve permitir que várias VPNs SSL sejam definidas simultaneamente
3.1.26.3. Deve permitir a personalização da porta TCP na qual a VPN SSL funciona
3.1.26.4. Deve permitir a autenticação usando nome de usuário e senha
3.1.26.5. Deve permitir a autenticação de dois fatores fornecida pelo mesmo fabricante
3.1.26.6. Deve permitir a autenticação usando certificados digitais
3.1.26.7. Para uso específico de VPN SSL (pelo menos):
3.1.26.8. Especificação IP do concentrador;
3.1.26.9. Especificação da porta do hub;
3.1.26.10. Deve suportar o uso de autenticação SAML (Security Assertion Markup Language) para os clientes que rodam na plataforma Microsoft Windows.

3.1.27. FUNCIONALIDADES DE GERECIAMENTO CENTRALIZADO

3.1.27.1. Deve permitir a instalação no Microsoft Windows Server 2012 R2, 2016 ou 2019;
3.1.27.2. O console de gerenciamento centralizado deve ser entregue sem custo;
3.1.27.3. Deve permitir a adição de clientes adicionando licenças.
3.1.27.4. Deve ter interface gráfica de gerenciamento
3.1.27.5. Deve ter funcionalidade de backup
3.1.27.6. Deve permitir a criação de usuários de diferentes perfis administrativos
3.1.27.7. Deve permitir importar informações do Active Directory usando LDAP
3.1.27.8. Deve permitir registro manual da estação através de um uso de uma senha
3.1.27.9. Deve permitir a criação de grupos de clientes para facilitar o gerenciamento
3.1.27.10. Deve permitir que a configuração do cliente mediante a definições em XML
3.1.27.11. Deve permitir que as configurações de perfil sejam importadas em um dispositivo de firewall do mesmo fabricante
3.1.27.12. Deve permitir a configuração de diferentes grupos e perfis para facilitar a administração
3.1.27.13. Deve permitir a configuração de antivírus, filtro da web, controle de aplicativos, verificador de vulnerabilidades e perfis de VPN
3.1.27.14. Deve permitir a proteção em tempo real
3.1.27.15. Deve permitir que a configuração de pesquisas de vírus e vulnerabilidades em uma base agendada
3.1.27.16. Deve permitir verificação completa e verificação rápida
3.1.27.17. Deve permitir que o usuário configure VPNs localmente
3.1.27.18. Deve permitir que o usuário desconecte uma VPN
3.1.27.19. Deve permitir a conexão VPN antes do login
3.1.27.20. Deve permitir conexão VPN automática
3.1.27.21. Deve suportar o uso específico ou geral para VPN IPSec (pelo menos)
3.1.27.22. Deve suportar o uso de certificados ou usuário e senha para autenticação
3.1.27.23. Deve suportar o uso de certificados no cartão inteligente
3.1.27.24. Deve suportar o bloqueio de tráfego IPv6
3.1.27.25. Deve suportar à opção para o usuário acessar a configuração do cliente por senha
3.1.27.26. Deve ser capaz de enviar logs para um sistema de log externos do mesmo fabricante
3.1.27.27. Dever permitir a instalação do certificado digital no cliente
3.1.27.28. Deve permitir ativar as funcionalidades de Logon Único
3.1.27.29. Deve ter informações disponíveis sobre: Número de dispositivos gerenciados, Versão do sistema operacional, Perfil aplicado, Usuário, Versão de assinatura do antivírus
3.1.27.30. Status do cliente de segurança: Registrado ou não registrado
3.1.27.31. Deve conter informações sobre o sistema operacional no qual o cliente está instalado
3.1.27.32. Deve informar o perfil de segurança criado e / ou aplicado
3.1.27.33. Deve informar os recursos de segurança aplicados: antivírus, filtro da web, VPN, firewall de aplicativo;
3.1.27.34. Deve permitir habilitar ou desabilitar os recursos antivírus, filtro da web, VPN, firewall de aplicativo nos terminais gerenciados
3.1.27.35. Deve ser capaz de fazer um inventário do software instalado em cada nó de extremidade
3.1.27.36. Deve permitir a implantação automática de clientes de terminal de acordo com a OU do MS AD ou grupos do MS AD

3.1.27.37. Deve permitir a manutenção de várias instâncias de instaladores com recursos diferentes (AV, VPN, WF, etc.) e arquiteturas (x86, x64, etc.)
3.1.27.38. Deve permitir a implantação de equipamentos que NÃO pertencem ao active directory (AD)
3.1.27.39. Deve permitir que regras de conformidade deficientes impeçam que um cliente mal configurado se conecte a redes críticas
3.1.27.40. Deve ser capaz de ser acessado através da administração WEB
3.1.27.41. Deve ter um painel em que possa verificar rapidamente o status de integridade dos clientes
3.1.27.42. Deve lidar com listas centralizadas de quarentena de arquivos
3.1.27.43. Deve poder aplicar políticas aos terminais de acordo com os grupos, para que os clientes pertencentes a esse grupo tenham a mesma política.
3.1.27.44. Deve poder aplicar políticas aos terminais de acordo com o usuário pertencente ao grupo, tornando mais granular à aplicação da política.
3.1.27.45. Deve poder atribuir configurações dinamicamente quando os clientes forem movidos dos grupos
3.1.27.46. As políticas de terminal devem atribuir perfis de proteção aos terminais. Esses perfis devem ser uma maneira de implantar uma configuração exclusiva de: malware, sandboxing, webfilter, firewall de aplicativos, VPN, verificação de vulnerabilidades e configurações do sistema (por exemplo, logfiels)
3.1.27.47. Os usuários administradores devem poder sincronizar com o AD, para permitir o login com as mesmas credenciais
3.1.27.48. Deve ser capaz de definir funções administrativas
3.1.27.49. Deve suportar fazer backup / restaurar configurações do console, configuração do servidor, políticas de terminal etc.
3.1.27.50. Funcionalidades de Provisionamento de Clientes
3.1.27.51. O fabricante deve fornecer um portal para baixar a segurança do cliente e permitir a instalação local
3.1.27.52. Deve ser compatível com a instalação via Microsoft Active Directory
3.1.27.53. O console de gerenciamento central deve poder instalar o cliente de segurança nos computadores Windows associados a um domínio da Microsoft
3.1.27.54. Deve suportar criação de várias versões de pacotes de instalação para serem associadas a grupos do Microsoft Active Directory.

3.1.28. VISIBILIDADE

3.1.28.1. Deve fornecer informações da estação de trabalho, no mínimo e não se limitando a: Nome completo, Telefone, E-mail, Informações pessoais obtidas minimamente de (entrada manual, linkedin, google, Sistema operacional e / ou salesforce), status do cliente, Nome do host, etiqueta de host
3.1.28.2. Deve suportar upload de uma foto ou avatar para identificação rápida do usuário
3.1.28.3. Deve relatar de maneira rápida e rápida, se fizer parte de um ambiente de segurança cooperativo
3.1.28.4. Deve relatar rapidamente o nível de vulnerabilidade da estação de trabalho
3.1.28.5. Deve ter um sistema de notificação pop-up
3.1.28.6. Deve ter uma lista de notificações atuais e anteriores
3.1.28.7. As notificações devem incluir: eventos AV, eventos ATP, eventos de comunicação, eventos de filtro da web e eventos do sistema.
3.1.28.8. Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas etc., bem como o CVE correspondente
3.1.28.9. Deve fornecer uma lista de aplicativos bloqueados
3.1.28.10. Caso o cliente fique em quarentena, deve ser capaz de informar ao usuário e notificar o gerenciamento.
3.1.28.11. Deve suportar a exibição de uma lista de explorações detectadas.
3.1.28.12. Deve permitir exibir uma lista de aplicativos protegidos contra exploração
3.1.28.13. Deve fornecer uma lista de arquivos em quarentena
3.1.28.14. Deve ser possível visualizar os resultados da análise ATP.

3.1.29. ANÁLISE DE VULNERABILIDADE

3.1.29.1. O cliente de segurança deve ter um módulo de pesquisa de vulnerabilidades integrado e permitir o gerenciamento central no console do mesmo fabricante
3.1.29.2. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda
3.1.29.3. As vulnerabilidades encontradas devem ser exibidas localmente com um link para visualizar informações de um banco de dados na Internet. deve ter pelo menos: nome, gravidade e detalhes
3.1.29.4. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas.

3.1.29.5. Links de acesso a informações complementares devem ser fornecidos, por exemplo, links para a página do fabricante onde as características da vulnerabilidade são detalhadas.
3.1.29.6. Deve permitir a aplicação automática de patches
3.1.29.7. Deve detalhar quais correções requerem instalação manual.
3.1.29.8. A verificação de vulnerabilidades deve ser permitida de maneira ordenada e autônoma a partir do console central
3.1.29.9. Deve verificar as vulnerabilidades antes de aplicar patches
3.1.30. FUNCIONALIDADES DE FILTRO DE CONTEÚDO WEB
3.1.30.1. Deve permitir a configuração do perfil de filtro da web a partir do console central do mesmo fabricante
3.1.30.2. O fabricante deve fazer consultas on-line com o cliente de segurança sobre a categoria de um determinado site (por exemplo, interesse geral, tecnologia, hackers, pornografia etc.) para aplicar a política de controle de acesso à Internet
3.1.30.3. O cliente de segurança deve suportar regras estáticas de acesso à Internet com base em expressões regulares
3.1.30.4. Para um determinada URL, os acessos devem ser: permitir, bloquear, alertar ou monitorar
3.1.30.5. Deve configurar o filtro de URL fornecido pelo fabricante com pelo menos as seguintes ações:
3.1.30.6. Bloquear, avisar, permitir e monitorar;
3.1.30.7. Deve configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as seguintes ações:
3.1.30.8. Bloquear ou permitir;

3.2. ITEM 02 – SOLUÇÃO PARA DUPLO FATOR DE AUTENTICAÇÃO - TOKEN MOBILE

3.2.1. Deve possuir 05 (cinco) licenciamentos perpétuos de token e sem limites de transferência para outros dispositivos.
3.2.2. Deve permitir o download gratuito nas lojas de aplicativos separado do seu provisionamento
3.2.3. O aplicativo deve suportar exclusão e adição de novos tokens
3.2.4. Deve ser instalado no dispositivo móvel sem que haja a necessidade de alteração de sua configuração, ou mesmo a capacidade de formatar o dispositivo móvel de forma remota
3.2.5. Deve garantir a privacidade do dispositivo móvel, ou seja, não deve ser capaz de consultar histórico de navegação
3.2.6. Deve requerer a permissão proprietário para envio de notificações ou qualquer tipo de alteração nas configurações
3.2.7. Deve suportar as principais plataformas de mobile do mercado (iOS (iPhone, iPod Touch, iPad), Android, Windows Phone 8, 8.1, Windows 10)
3.2.8. Deve suportar a geração dinâmica das sementes de token, minimizando a exposição online.
3.2.9. Deve suportar ativação através da utilização de QR Codes e manual
3.2.10. Deve criptografar o armazenamento de sementes utilizadas na geração do token
3.2.11. Deve ser capaz de gerar senhas de uso único (One Time Programmable - OTP) baseado em tempo (TOTP) ou evento (HTOP) compatível com OATH
3.2.12. Deve suportar a ocultação do token para tokens baseados em tempo (TOTP)
3.2.13. Deve capaz de proteger abertura do aplicativo através de PIN ou Impressão Digital ou Face Security
3.2.14. Deve exibir o intervalo de tempo OTP
3.2.15. Deve exibir do número de série do token
3.2.16. Deve ser compatível com o relógio da Apple
3.2.17. Deve suportar que a senha gerada possa ser copiada para a área de transferência
3.2.18. Deve suportar detalhes de login enviados ao telefone para aprovação com um toque
3.2.19. Deve usar um serviço de provisionamento dinâmico, onde apenas na atribuição de um token a um usuário a semente é criada e é removida durante o download ou após um tempo limite configurável.
3.2.20. Deve ser compatível e permitir integração com atual "SOLUÇÃO AUTENTICAÇÃO E GERENCIAMENTO DE ACESSO" existente na PRODEB, e com itens "SOLUÇAO DE SEGURANÇA DE REDE NGFW TIPO I, II"
3.2.21. Deve estar de acordo com as seguintes RFCs para especificações OTP: RFC6238 e RFC4226
3.2.22. Deve ser capaz de realizar vinculação com o dispositivo móvel
3.2.23. Deve suportar à sua utilização como segundo fator de autenticação para acesso VPN via SSL ou IPSEC, sem a necessidade de utilização de um servidor Radius
3.2.24. Deve ser compatível com Google, Dropbox, Amazon e outros tokens TOTP (Time-based One-Time Password) compatíveis com OAT.

3.3. ITEM 03 – SOLUÇAO DE SEGURANÇA DE REDE NGFW TIPO I

3.3.1. CARACTERISTICAS GERAIS:

3.3.1.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

3.3.1.2. 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, desde que ocupem até 2U, no máximo.

3.3.1.3. A solução deverá ser fornecida com licenças para utilização durante a vigência contratual de 24 (vinte e quatro)meses, com as funcionalidades habilitadas de Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações.

3.3.1.4. Deve possuir fonte de alimentação com chaveamento automático 110/220V.

3.3.1.5. Deve possuir firewall com capacidade mínima de processamento de 6 (seis) Gbps.

3.3.1.6. Deve possuir IPS com capacidade mínima de processamento de 1 (um) Gbps.

3.3.1.7. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 600 (seiscentos) Mbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

3.3.1.8. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 600 (seiscentos) Mbps.

3.3.1.9. Deve possuir VPN com capacidade de, pelo menos, 06 (seis) Gbps de tráfego IPSec.

3.3.1.10. Deve suportar 600.000 (seiscentos mil) conexões simultâneas.

3.3.1.11. Deverão ser licenciados para suportar, pelo menos, 200 (duzentos) usuários de VPN SSL.

3.3.1.12. Deve suportar, pelo menos, 30.000 (trinta mil) novas conexões por segundo.

3.3.1.13. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.

3.3.1.14. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Client-Site.

3.3.1.15. Deve possuir, pelo menos, 08 (oito) interfaces RJ 45.

3.3.1.16. Deve ser fornecida Solução de Gerência Centralizada de Equipamentos, caso compatível poderá ser utilizada atual solução existente na PRODEB, Marca Fortinet, Modelo FMG-3000G.

3.3.1.17. Deve ser fornecida Solução Centralizada de Armazenamento de Logs e Relatórios, caso compatível poderá ser utilizada atual solução existente na PRODEB, Marca Fortinet, Modelo FAZ-3700G.

3.3.1.18. deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

3.3.1.19. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

3.3.2. FUNCIONALIDADE DE FIREWALL

3.3.2.1. Deve possuir controle de acesso à internet por endereço IP de origem e destino;

3.3.2.2. Deve possuir controle de acesso à internet por sub rede;

3.3.2.3. Deve suportar tags de VLAN (802.1q);

3.3.2.4. Deve possuir ferramenta de diagnóstico do tipo tcpdump;

3.3.2.5. Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

3.3.2.6. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

3.3.2.7. Deve suportar single-sign-on para Active Directory, RADIUS;

3.3.2.8. Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

3.3.2.9. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

3.3.2.10. Deve permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

3.3.2.11. Deve permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

3.3.2.12. Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

3.3.2.13. Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

3.3.2.14. Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;

3.3.2.15. Deve suportar aplicações multimídia, como: H.323 e SIP;

3.3.2.16. Deve possuir tecnologia de firewall do tipo Statefull;

3.3.2.17. Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
3.3.2.18. Deve permitir o funcionamento em modo transparente tipo "bridge" sem alterar o endereço MAC do tráfego;
3.3.2.19. Deve suportar PBR – Policy Based Routing;
3.3.2.20. Deve permitir a criação de VLANS no padrão IEEE 802.1q;
3.3.2.21. Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
3.3.2.22. Deve permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;
3.3.2.23. Deve permitir forwarding de camada 2 para protocolos não IP;
3.3.2.24. Deve suportar forwarding multicast;
3.3.2.25. Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;
3.3.2.26. Deve permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;
3.3.2.27. Deve permitir o agrupamento de serviços;
3.3.2.28. Deve permitir o filtro de pacotes sem a utilização de NAT;
3.3.2.29. Deve permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
3.3.2.30. Deve possuir mecanismo de anti-spoofing;
3.3.2.31. Deve permitir criação de regras definidas pelo usuário;
3.3.2.32. Deve permitir o serviço de autenticação para tráfego HTTP e FTP;
3.3.2.33. Deve permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;
3.3.2.34. Deve possuir a funcionalidade de balanceamento e contingência de links;
3.3.2.35. Deve suportar sFlow;
3.3.2.36. O dispositivo deve ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas.
3.3.2.37. Deve ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;
3.3.2.38. Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
3.3.2.39. Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;
3.3.2.40. Deve suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;
3.3.2.41. Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;
3.3.2.42. Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;
3.3.2.43. Deve suportar SIP, H.323 e SCCP NAT Traversal;
3.3.2.44. Deve permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;
3.3.2.45. Deve possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

3.3.3. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

3.3.3.1. 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;
3.3.3.2. Deve permitir modificação de valores DSCP para o DiffServ;
3.3.3.3. Deve permitir priorização de tráfego e suportar ToS;
3.3.3.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;
3.3.3.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
3.3.3.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

3.3.3.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
3.3.3.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;
3.3.3.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;
3.3.3.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;
3.3.4. FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY
3.3.4.1. Deve permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;
3.3.4.2. Deve possuir filtragem de e-mail por palavras chaves;
3.3.4.3. Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
3.3.4.4. Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL;
3.3.4.5. Deve permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;
3.3.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB
3.3.5.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;
3.3.5.2. Deve possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;
3.3.5.3. Deve possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;
3.3.5.4. Deve possuir a funcionalidade de cota de tempo de utilização por categoria;
3.3.5.5. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:
3.3.5.5.1. Proxy anônimo;
3.3.5.5.2. Webmail;
3.3.5.5.3. Instituições de saúde;
3.3.5.5.4. Notícias;
3.3.5.5.5. Phishing;
3.3.5.5.6. Hackers;
3.3.5.5.7. Pornografia;
3.3.5.5.8. Racismo;
3.3.5.5.9. Websites pessoais;
3.3.5.5.10. Compras;
3.3.5.6. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
3.3.5.7. Deve permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;
3.3.5.8. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;
3.3.5.9. 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;
3.3.5.10. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
3.3.5.11. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
3.3.5.12. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
3.3.5.13. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;
3.3.5.14. Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;
3.3.5.15. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;
3.3.5.16. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);
3.3.5.17. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;
3.3.5.18. Deve filtrar o conteúdo baseado em categorias em tempo real;
3.3.5.19. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;
3.3.5.20. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

3.3.5.21. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
3.3.5.22. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem;
3.3.5.23. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;
3.3.5.24. Deve permitir o bloqueio de redirecionamento HTTP;
3.3.5.25. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;
3.3.5.26. Deve possuir Proxy Explícito e Transparente;
3.3.5.27. Deve implementar roteamento WCCP e ICAP;

3.3.6. FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

3.3.6.1. 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;
3.3.6.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;
3.3.6.3. Deve estar orientado à proteção de redes;
3.3.6.4. Deve permitir funcionar em modo transparente, sniffer e router;
3.3.6.5. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
3.3.6.6. Deve permitir a criação de padrões de ataque manualmente;
3.3.6.7. Deve possuir integração à plataforma de segurança;
3.3.6.8. Deve possuir capacidade de remontagem de pacotes para identificação de ataques;
3.3.6.9. 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;
3.3.6.10. 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;
3.3.6.11. Deve possuir mecanismos de detecção/proteção de ataques;
3.3.6.12. Deve possuir reconhecimento de padrões;
3.3.6.13. Deve possuir análise de protocolos;
3.3.6.14. Deve possuir detecção de anomalias;
3.3.6.15. Deve possuir detecção de ataques de RPC (Remote Procedure Call);
3.3.6.16. Deve possuir proteção contra-ataques de Windows ou NetBios;
3.3.6.17. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);
3.3.6.18. Deve possuir proteção contra-ataques DNS (Domain Name System);
3.3.6.19. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;
3.3.6.20. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);
3.3.6.21. Deve possuir métodos de notificação de detecção de ataques;
3.3.6.22. Deve possuir alarmes na console de administração;
3.3.6.23. Deve possuir alertas via correio eletrônico;
3.3.6.24. 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;
3.3.6.25. Deve ter a capacidade de resposta/logs ativa a ataques;
3.3.6.26. Deve prover a terminação de sessões via TCP resets;
3.3.6.27. Deve armazenar os logs de sessões;
3.3.6.28. Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
3.3.6.29. Deve mitigar os efeitos dos ataques de negação de serviços;
3.3.6.30. Deve permitir a criação de assinaturas personalizadas;
3.3.6.31. Deve possuir filtros de ataques por anomalias;
3.3.6.32. Deve permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
3.3.6.33. Deve permitir filtros de anomalias de protocolos;
3.3.6.34. Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
3.3.6.35. Deve suportar verificação de ataque na camada de aplicação;
3.3.6.36. Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;
3.3.6.37. Deve possuir as seguintes estratégias de bloqueio: pass, drop e reset.

3.3.7. FUNCIONALIDADE DE VPN

3.3.7.1. Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

3.3.7.2. Deve possuir suporte a certificados PKI X.509 para construção de VPNs;
3.3.7.3. Deve possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;
3.3.7.4. Deve possuir suporte a VPN SSL;
3.3.7.5. Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
3.3.7.6. Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;
3.3.7.7. A VPN SSL deve suportar cliente para plataforma Windows, Linux e Mac OS X;
3.3.7.8. Deve permitir a arquitetura de VPN hub and spoke;
3.3.7.9. Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

3.3.8. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
3.3.8.1. Deve reconhecer, no mínimo, 2.000 (duas mil) aplicações;
3.3.8.2. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;
3.3.8.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:
3.3.8.3.1. P2P
3.3.8.3.2. Instant Messaging;
3.3.8.3.3. Web client;
3.3.8.3.4. Transferência de arquivos;
3.3.8.3.5. VoIP;
3.3.8.4. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
3.3.8.5. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
3.3.8.6. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
3.3.8.7. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
3.3.8.8. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
3.3.8.9. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
3.3.8.10. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
3.3.8.11. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
3.3.8.12. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
3.3.8.13. Deve permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;
3.3.8.14. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;
3.3.8.15. Deve permitir criação de padrões de aplicação manualmente;

3.3.9. FUNCIONALIDADE DE BALANCEAMENTO DE CARGA
3.3.9.1. Deve permitir a criação de endereços IPs virtuais;
3.3.9.2. Deve suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;
3.3.9.3. Deve permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;
3.3.9.4. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;
3.3.9.5. Deve permitir que seja mantido o IP de origem;
3.3.9.6. Deve suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;
3.3.9.7. Deve ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;
3.3.9.8. Deve permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

3.3.10. FUNCIONALIDADE DE SD-WAN
3.3.10.1. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.
3.3.10.2. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.
3.3.10.3. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.
3.3.10.4. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

3.3.10.5. Solução deve ser capaz de prover Zero Touch provisioning.
3.3.10.6. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.
3.3.10.7. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.
3.3.10.8. A solução deve ser capaz de criar VPN "Full-Mesh" em interface gráfica ou CLI, de forma automática, e sem que o administrador precise configurar site por site.
3.3.10.9. A configuração VPN IPSEC deve oferecer suporte para DH Group: 14 e 15.
3.3.10.10. Reconhecimento em camada 7 totalmente segregado da camada 4.
3.3.10.11. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.
3.3.10.12. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
3.3.10.13. Ainda 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)
3.3.10.14. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6
3.3.10.15. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.
3.3.10.16. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.
3.3.10.17. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de saúde melhor que o link atual.
3.3.10.18. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.
3.3.10.19. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

3.4. ITEM 04 – SOLUÇAO DE SEGURANÇA DE REDE NGFW TIPO II

3.4.1. CARACTERISTICAS GERAIS:

3.4.1.1. A solução deve ser entregue no formato de solução virtual, compatível com as plataformas VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, a responsabilidade pelo fornecimento e a implantação de servidor/hardware com licenciamento necessário será da CONTRATADA, e o equipamento deve ser instalado no local indicado pela CONTRATANTE.
3.4.1.2. A solução deverá ser fornecida com licenças para utilização durante a vigência contratual de 24 (vinte e quatro)meses, com as funcionalidades habilitadas de Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações.
3.4.1.3. Deve suportar e possuir licenciamento para até 04 vCPU.
3.4.1.4. Deve suportar e possuir licenciamento para no mínimo 02 GB de Memória.
3.4.1.5. Deve suportar e possuir licenciamento para até 10 interfaces de rede.
3.4.1.6. Deve possuir firewall com capacidade mínima de processamento de 2 (dois) Gbps.
3.4.1.7. Deve possuir IPS com capacidade mínima de processamento de 3 (três) Gbps.
3.4.1.8. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1,7 (um virgula sete) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.
3.4.1.9. Deve possuir VPN com capacidade de, pelo menos, 2 (dois) Gbps de tráfego IPSec.
3.4.1.10. Deve suportar 5.000.000 (cinco milhões) conexões simultâneas.
3.4.1.11. Deve suportar, pelo menos, 100.000 (cem mil) novas conexões por segundo.
3.4.1.12. Deve ser fornecida Solução de Gerência Centralizada de Equipamentos, caso compatível poderá ser utilizada atual solução existente na PRODEB, Marca Fortinet, Modelo FMG-3000G.
3.4.1.13. Deve ser fornecida Solução Centralizada de Armazenamento de Logs e Relatórios, caso compatível poderá ser utilizada atual solução existente na PRODEB, Marca Fortinet, Modelo FAZ-3700G.

3.4.1.14. deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

3.4.1.15. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

3.4.2. FUNCIONALIDADE DE FIREWALL

3.4.2.1. Deve possuir controle de acesso à internet por endereço IP de origem e destino;

3.4.2.2. Deve possuir controle de acesso à internet por sub rede;

3.4.2.3. Deve suportar tags de VLAN (802.1q);

3.4.2.4. Deve possuir ferramenta de diagnóstico do tipo tcpdump;

3.4.2.5. Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

3.4.2.6. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

3.4.2.7. Deve suportar single-sign-on para Active Directory, RADIUS;

3.4.2.8. Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

3.4.2.9. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

3.4.2.10. Deve permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

3.4.2.11. Deve permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

3.4.2.12. Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

3.4.2.13. Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

3.4.2.14. Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;

3.4.2.15. Deve suportar aplicações multimídia, como: H.323 e SIP;

3.4.2.16. Deve possuir tecnologia de firewall do tipo Statefull;

3.4.2.17. Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

3.4.2.18. Deve permitir o funcionamento em modo transparente tipo "bridge" sem alterar o endereço MAC do tráfego;

3.4.2.19. Deve suportar PBR – Policy Based Routing;

3.4.2.20. Deve permitir a criação de VLANS no padrão IEEE 802.1q;

3.4.2.21. Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

3.4.2.22. Deve permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

3.4.2.23. Deve permitir forwarding de camada 2 para protocolos não IP;

3.4.2.24. Deve suportar forwarding multicast;

3.4.2.25. Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;

3.4.2.26. Deve permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

3.4.2.27. Deve permitir o agrupamento de serviços;

3.4.2.28. Deve permitir o filtro de pacotes sem a utilização de NAT;

3.4.2.29. Deve permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

3.4.2.30. Deve possuir mecanismo de anti-spoofing;

3.4.2.31. Deve permitir criação de regras definidas pelo usuário;

3.4.2.32. Deve permitir o serviço de autenticação para tráfego HTTP e FTP;

3.4.2.33. Deve permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

3.4.2.34. Deve possuir a funcionalidade de balanceamento e contingência de links;

3.4.2.35. Deve suportar sFlow;

3.4.2.36. O dispositivo deve ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas.

3.4.2.37. Deve ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

3.4.2.38. Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

3.4.2.39. Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;
3.4.2.40. Deve suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;
3.4.2.41. Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;
3.4.2.42. Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;
3.4.2.43. Deve suportar SIP, H.323 e SCCP NAT Traversal;
3.4.2.44. Deve permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;
3.4.2.45. Deve possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

3.4.3. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO
3.4.3.1. 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;
3.4.3.2. Deve permitir modificação de valores DSCP para o DiffServ;
3.4.3.3. Deve permitir priorização de tráfego e suportar ToS;
3.4.3.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;
3.4.3.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
3.4.3.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
3.4.3.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
3.4.3.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;
3.4.3.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;
3.4.3.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

3.4.4. FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY
3.4.4.1. Deve permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;
3.4.4.2. Deve possuir filtragem de e-mail por palavras chaves;
3.4.4.3. Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
3.4.4.4. Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL;
3.4.4.5. Deve permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

3.4.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB
3.4.5.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;
3.4.5.2. Deve possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;
3.4.5.3. Deve possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;
3.4.5.4. Deve possuir a funcionalidade de cota de tempo de utilização por categoria;
3.4.5.5. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:
3.4.5.5.1. Proxy anônimo;
3.4.5.5.2. Webmail;
3.4.5.5.3. Instituições de saúde;
3.4.5.5.4. Notícias;
3.4.5.5.5. Phishing;
3.4.5.5.6. Hackers;
3.4.5.5.7. Pornografia;
3.4.5.5.8. Racismo;
3.4.5.5.9. Websites pessoais;
3.4.5.5.10. Compras;
3.4.5.6. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
3.4.5.7. Deve permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;

3.4.5.8. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;
3.4.5.9. 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;
3.4.5.10. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
3.4.5.11. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
3.4.5.12. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
3.4.5.13. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;
3.4.5.14. Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;
3.4.5.15. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;
3.4.5.16. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);
3.4.5.17. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;
3.4.5.18. Deve filtrar o conteúdo baseado em categorias em tempo real;
3.4.5.19. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;
3.4.5.20. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
3.4.5.21. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
3.4.5.22. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem;
3.4.5.23. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;
3.4.5.24. Deve permitir o bloqueio de redirecionamento HTTP;
3.4.5.25. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;
3.4.5.26. Deve possuir Proxy Explícito e Transparente;
3.4.5.27. Deve implementar roteamento WCCP e ICAP;

3.4.6. FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

3.4.6.1. 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;
3.4.6.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;
3.4.6.3. Deve estar orientado à proteção de redes;
3.4.6.4. Deve permitir funcionar em modo transparente, sniffer e router;
3.4.6.5. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
3.4.6.6. Deve permitir a criação de padrões de ataque manualmente;
3.4.6.7. Deve possuir integração à plataforma de segurança;
3.4.6.8. Deve possuir capacidade de remontagem de pacotes para identificação de ataques;
3.4.6.9. 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;
3.4.6.10. 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;
3.4.6.11. Deve possuir mecanismos de detecção/proteção de ataques;
3.4.6.12. Deve possuir reconhecimento de padrões;
3.4.6.13. Deve possuir análise de protocolos;
3.4.6.14. Deve possuir detecção de anomalias;
3.4.6.15. Deve possuir detecção de ataques de RPC (Remote Procedure Call);
3.4.6.16. Deve possuir proteção contra-ataques de Windows ou NetBios;
3.4.6.17. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

3.4.6.18. Deve possuir proteção contra-ataques DNS (Domain Name System);
3.4.6.19. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;
3.4.6.20. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);
3.4.6.21. Deve possuir métodos de notificação de detecção de ataques;
3.4.6.22. Deve possuir alarmes na console de administração;
3.4.6.23. Deve possuir alertas via correio eletrônico;
3.4.6.24. 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;
3.4.6.25. Deve ter a capacidade de resposta/logs ativa a ataques;
3.4.6.26. Deve prover a terminação de sessões via TCP resets;
3.4.6.27. Deve armazenar os logs de sessões;
3.4.6.28. Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
3.4.6.29. Deve mitigar os efeitos dos ataques de negação de serviços;
3.4.6.30. Deve permitir a criação de assinaturas personalizadas;
3.4.6.31. Deve possuir filtros de ataques por anomalias;
3.4.6.32. Deve permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
3.4.6.33. Deve permitir filtros de anomalias de protocolos;
3.4.6.34. Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
3.4.6.35. Deve suportar verificação de ataque na camada de aplicação;
3.4.6.36. Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;
3.4.6.37. Deve possuir as seguintes estratégias de bloqueio: pass, drop e reset.

3.4.7. FUNCIONALIDADE DE VPN
3.4.7.1. Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
3.4.7.2. Deve possuir suporte a certificados PKI X.509 para construção de VPNs;
3.4.7.3. Deve possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;
3.4.7.4. Deve possuir suporte a VPN SSL;
3.4.7.5. Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
3.4.7.6. Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;
3.4.7.7. A VPN SSL deve suportar cliente para plataforma Windows, Linux e Mac OS X;
3.4.7.8. Deve permitir a arquitetura de VPN hub and spoke;
3.4.7.9. Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

3.4.8. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
3.4.8.1. Deve reconhecer, no mínimo, 2.000 (duas mil) aplicações;
3.4.8.2. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;
3.4.8.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:
3.4.8.3.1. P2P
3.4.8.3.2. Instant Messaging;
3.4.8.3.3. Web client;
3.4.8.3.4. Transferência de arquivos;
3.4.8.3.5. VoIP;
3.4.8.4. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
3.4.8.5. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
3.4.8.6. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
3.4.8.7. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
3.4.8.8. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
3.4.8.9. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
3.4.8.10. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
3.4.8.11. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
3.4.8.12. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

3.4.8.13. Deve permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;

3.4.8.14. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

3.4.8.15. Deve permitir criação de padrões de aplicação manualmente;

3.4.9. FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

3.4.9.1. Deve permitir a criação de endereços IPs virtuais;

3.4.9.2. Deve suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

3.4.9.3. Deve permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;

3.4.9.4. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;

3.4.9.5. Deve permitir que seja mantido o IP de origem;

3.4.9.6. Deve suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

3.4.9.7. Deve ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

3.4.9.8. Deve permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

3.4.10. FUNCIONALIDADE DE SD-WAN

3.4.10.1. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

3.4.10.2. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

3.4.10.3. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

3.4.10.4. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

3.4.10.5. Solução deve ser capaz de prover Zero Touch provisioning.

3.4.10.6. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

3.4.10.7. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

3.4.10.8. A solução deve ser capaz de criar VPN "Full-Mesh" em interface gráfica ou CLI, de forma automática, e sem que o administrador precise configurar site por site.

3.4.10.9. A configuração VPN IPSEC deve oferecer suporte para DH Group: 14 e 15.

3.4.10.10. Reconhecimento em camada 7 totalmente segregado da camada 4.

3.4.10.11. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.

3.4.10.12. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

3.4.10.13. Ainda 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)

3.4.10.14. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6

3.4.10.15. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.

3.4.10.16. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

3.4.10.17. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de saúde melhor que o link atual.

3.4.10.18. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

3.4.10.19. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

3.5. ITEM 05 – SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAF TIPO I

3.5.1. CARACTERÍSTICAS E FUNCIONALIDADES GERAIS

3.5.1.1. A solução deve ser entregue em appliance ou no formato de solução virtual, compatível com as plataformas VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, no caso de solução virtualizada a responsabilidade pela implantação de servidor/hardware com licenciamento necessário será da CONTRATADA, e o equipamento deve ser instalado no local indicado pela CONTRATANTE.

3.5.1.2. Poderá ser entregue em equipamento único ou com composição de equipamentos. para atender as funcionalidades exigidas.

3.5.1.3. A solução deverá ser fornecida com licenças para utilização durante a vigência contratual de 24 (vinte e quatro) meses, com as funcionalidades habilitadas de AV, IPS, WAF Security Service, IP Reputation, Sandbox, Credential Stuffing Defense Service.

3.5.2. Requisitos Mínimos de Performance

3.5.2.1. Deve possuir throughput mínimo para HTTP de 450 (quatrocentos e cinquenta) Mbps;

3.5.2.2. Deve suportar quantidade ilimitada de aplicações protegidas;

3.5.2.3. Deve suportar até 10 interfaces de rede;

3.5.2.4. Deve suportar até 04 vCPU;

3.5.3. Requisitos Mínimos de Funcionalidades

3.5.3.1. Todos os equipamentos que compõem a solução devem ser entregues com a última versão de software homologada e recomendada pelo fabricante.

3.5.3.2. Deve ser fornecida Solução Centralizada de Armazenamento de Logs e Relatórios, caso compatível poderá ser utilizada atual solução existente na PRODEB, Marca Fortinet, Modelo FAZ-3700G.

3.5.3.3. A solução proposta deve contemplar para a solução de armazenamento, análise de logs e relatoria o projeto de implantação, migração, garantia, capacitação da equipe local e suporte.

3.5.4. Funcionalidades de Rede

3.5.4.1. A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso), Passivo, ou "Sniffer"

3.5.4.2. (Offline) e Inline Transparente (Bridge).

3.5.4.3. A solução deve ser capaz de ser implementada com protocolo WCCP.

3.5.4.4. Suportar VLANs no padrão IEEE 802.1q.

3.5.4.5. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP) - IEEE 802.3ad.

3.5.4.6. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs).

3.5.4.7. A solução deve suportar roteamento por política (policy route).

3.5.4.8. Funcionalidades de Gerência

3.5.4.9. O sistema operacional / firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, e através de CLI (interface de linha de comando), acessando localmente, via porta de console, ou remotamente via SSH.

3.5.4.10. Deve possuir administração baseada em interface web HTTPS.

3.5.4.11. Possuir auto-complementação de comandos na CLI.

3.5.4.12. Possuir ajuda contextual na CLI.

3.5.4.13. A solução deve possuir Interface Gráfica com informações sobre o sistema Ex: (Informações do Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware).

3.5.4.14. Deve ser possível visualizar através da interface gráfica de gerência informações de licenças e assinaturas.

3.5.4.15. Deve prover, na interface de gerência, as seguintes informações do sistema para cada gateway: consumo de CPU e estatísticas das conexões.

3.5.4.16. Deve ser possível visualizar na interface de gerência as informações de consumo de memória.

3.5.4.17. Deve ser possível visualizar na interface de gerência ou CLI as informações de utilização de disco de log.

3.5.4.18. Deve possuir ferramenta, na interface gráfica de gerência (dashboard) que permita visualizar os últimos logs de ataque detectados/bloqueados.

3.5.4.19. Deve prover as seguintes informações, na interface de gráfica de gerência: estatísticas de throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema.
3.5.4.20. Possuir na interface gráfica estatísticas de conexões concorrentes e por segundo, de políticas de segurança do sistema.
3.5.4.21. Possuir um painel de visualização com informações das interfaces de rede do sistema.
3.5.4.22. A configuração de administração da solução deve possibilitar a utilização de perfis.
3.5.4.23. Deve ser possível executar e restaurar backup via interface Web (GUI).
3.5.4.24. Deve ter a opção para criptografar o backup.
3.5.4.25. Deve ser possível executar e restaurar backup utilizando-se um ou mais dos seguintes protocolos: FTP, SFTP ou TFTP,ou HTTPS
3.5.4.26. Deve ser possível instalar um firmware alternativo em disco e inicializá-lo manualmente em caso de falha do firmware principal.
3.5.4.27. Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3.
3.5.4.28. Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog.
3.5.4.29. A solução deve ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG.
3.5.4.30. Ter a capacidade de armazenar logs em appliance remoto.
3.5.4.31. A solução deve ter a capacidade de adicionar identificadores customizados nos registros syslog antes de envio, como hostname, atrelados a valores fixos ou variáveis.
3.5.4.32. A solução deve ter a capacidade de enviar alertas por e-mail de eventos baseados em severidades e/ou categorias.
3.5.4.33. A solução deve possuir dados analíticos contendo localização geográfica dos clientes web.
3.5.4.34. A solução deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem, o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (hits) e percentual de cada país de origem.
3.5.4.35. Deve ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário.
3.5.4.36. Deve ter suporte a RESTful API para gerenciamento de configurações.
3.5.4.37. Deve suportar todas as funcionalidades para comunicação HTTP/2

3.5.5. Funcionalidades de Autenticação
3.5.5.1. Os usuários devem ser capazes de autenticar através do cabeçalho de autorização HTTP / HTTPS.
3.5.5.2. Os usuários devem ser capazes de autenticar através de formulários HTML embutidos.
3.5.5.3. A solução deve ser capaz de autenticar usuários através de certificados digitais pessoais.
3.5.5.4. Deve possuir base local para armazenamento e autenticação contas de usuários.
3.5.5.5. A solução deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS.
3.5.5.6. Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM.
3.5.5.7. A solução deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação.

3.5.6. Funcionalidades de Web Application Firewall
3.5.6.1. 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.
3.5.6.2. Deve implementar recursos de Sandbox para análise de malware moderno;
3.5.6.3. 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.
3.5.6.4. Deve implementar proteção contra a lista de técnicas/ataques listados no OWASP 10 (Open Web Application security Project)
3.5.6.5. 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.
3.5.6.6. Ter a capacidade de criação de assinaturas de ataque customizáveis.
3.5.6.7. Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol.
3.5.6.8. Ter a capacidade de proteção para ataques do tipo Botnet.
3.5.6.9. Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST).
3.5.6.10. A solução deve possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta.

3.5.6.11. Deve suportar detecção a ataques de Clickjacking.
3.5.6.12. Deve suportar detecção a ataques de alteração de cookie.
3.5.6.13. Deve identificar e prevenir ataques do tipo Credit Card Theft.
3.5.6.14. Deve identificar e prevenir ataque Cross Site Request Forgery (CSRF).
3.5.6.15. A solução deve possuir funcionalidade de proteção positiva contra ataques como cross site scripting (XSS).
3.5.6.16. Deve possuir proteção contra ataques de Denial of Service (DoS).
3.5.6.17. Deve possuir a capacidade de proteção para ataques do tipo HTTP header overflow.
3.5.6.18. Deve possuir a capacidade de proteção para ataques do tipo Local File inclusion (FLI).
3.5.6.19. Deve possuir a capacidade de proteção para ataques do tipo Man-in-the-middle (MITM).
3.5.6.20. Deve possuir a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI).
3.5.6.21. Deve possuir a capacidade de proteção para ataques do tipo Server Information Leakage.
3.5.6.22. Deve possuir proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection).
3.5.6.23. Deve possuir a capacidade de proteção para ataques do tipo Malformed XML.
3.5.6.24. Deve Identificar e prevenir ataques do tipo Low-rate DoS.
3.5.6.25. Deve possuir prevenção contra Slow POST attack.
3.5.6.26. Deve proteger contra ataques Slowloris.
3.5.6.27. Deve possuir a capacidade de proteção para ataques do tipo SYN flood.
3.5.6.28. Deve possuir a capacidade de proteção para ataques do tipo Forms Tampering.
3.5.6.29. A solução deve possuir funcionalidade de proteção positiva contra ataques de manipulação de campo escondido.
3.5.6.30. Deve possuir a capacidade de proteção para ataques do tipo Directory Traversal.
3.5.6.31. Deve possuir a capacidade de proteção do tipo Access Rate Control.
3.5.6.32. 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.
3.5.6.33. Deve permitir configurar regras de bloqueio a métodos HTTP indesejados.
3.5.6.34. Deve permitir que sejam configuradas regras de limite de upload por tamanho de arquivo.
3.5.6.35. 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.
3.5.6.36. Deve permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem.
3.5.6.37. Deve permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.
3.5.6.38. Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation.
3.5.6.39. Deve possuir a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP.
3.5.6.40. Deve possuir a funcionalidade de proteger o website contra ações de desfiguração (defacement), com restauração automática e rápida do site caso ocorra à falha.
3.5.6.41. Deve possuir a funcionalidade de antivírus para inspeção de tráfego e arquivos.
3.5.6.42. Deve possuir a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não-conformidade.
3.5.6.43. 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.
3.5.6.44. A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego.
3.5.6.45. Deve para SSL/TLS offload suportar no mínimo TLS 1.0, 1.1, 1.2 e 1.3.
3.5.6.46. A solução deve ter a capacidade de armazenar certificados digitais de CA's.
3.5.6.47. A solução deve ser capaz de gerar CSR para ser assinado por uma CA.
3.5.6.48. A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL).
3.5.6.49. 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.
3.5.6.50. 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.

3.5.6.51. A solução deve ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores.
3.5.6.52. 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.
3.5.6.53. 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).
3.5.6.54. A solução deve ter a capacidade de definir restrições a métodos HTTP.
3.5.6.55. A solução deve ter a capacidade de proteger contra a detecção de campos ocultos.
3.5.6.56. Deve permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares.
3.5.6.57. 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,
3.5.6.58. Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros.
3.5.6.59. A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML.
3.5.6.60. A solução deve permitir a exclusão de URLs na análise de vulnerabilidades.
3.5.6.61. Deve ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente.
3.5.6.62. Deve suportar redireção e reescrita de requisições e respostas HTTP.
3.5.6.63. Deve permitir redirecionar requisições HTTP para HTTPS.
3.5.6.64. Deve permitir reescrever a linha URL no cabeçalho de uma requisição HTTP.
3.5.6.65. Deve permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP.
3.5.6.66. Deve permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP.
3.5.6.67. Deve permitir redirecionar requisições para outro web site.
3.5.6.68. Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP.
3.5.6.69. Deve permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web.
3.5.6.70. Deve permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor web.
3.5.6.71. Deve permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso.
3.5.6.72. 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).
3.5.6.73. 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.
3.5.6.74. Possuir capacidade de caching para aceleração web.
3.5.6.75. Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.
3.5.6.76. Deve suportar no mínimo 500 regras de reescrita URL distintas
3.5.6.77. Deve suportar no mínimo 250 políticas de assinatura distintas
3.5.6.78. Deve suportar no mínimo 500 grupos ou pools de servidores, e cada pool deve suportar no mínimo 1000 membros
3.5.6.79. Deve suportar no mínimo 1000 IPs virtuais configurados e ativos simultaneamente
3.5.6.80. Deve ser capaz de restringir acesso quando as requisições não tiverem um cabeçalho HTTP específico pré-configurado.
3.5.6.81. Deve ser capaz de limitar o número de usuários/origens simultâneos acessando a mesma conta/sessão/login.
3.5.6.82. 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.
3.5.6.83. Deve ser capaz de adicionar múltiplos servidores ADFS em um pool de servidores
3.5.6.84. 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.

3.5.7. Outras funcionalidades

3.5.7.1. A solução deve incluir funcionalidade de balanceamento de carga entre servidores web.
3.5.7.2. Deve possuir a habilidade de configurar portas não-padrão para aplicação web HTTP e HTTPS.

3.5.7.3. Deve possuir a capacidade de balancear/distribuir tráfego e rotear o conteúdo através de vários servidores web.
3.5.7.4. A solução deve permitir criar grupos de servidores (Server Farm / Pool) para distribuir as conexões dos usuários.
3.5.7.5. Deve suportar algoritmo Round Robin para balanceamento de carga de servidores.
3.5.7.6. Deve suportar algoritmo Weighted Round Robin para balanceamento de carga de servidores.
3.5.7.7. Deve suportar algoritmo Least Connections para balanceamento de carga de servidores.
3.5.7.8. A solução deve ser capaz de criar servidores virtuais que definem a interface de rede/bridge e endereço IP por onde o tráfego destinado ao Server Pool é recebido.
3.5.7.9. Os servidores virtuais devem entregar o tráfego à um único servidor web e também possuir a opção de distribuir as sessões/conexões entre os servidores web do Server Pool.
3.5.7.10. Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do Server Pool.
3.5.7.11. Deve permitir teste de disponibilidade de servidor web através do método TCP.
3.5.7.12. Deve permitir teste de disponibilidade de servidor web através do método ICMP ECHO_REQUEST (ping).
3.5.7.13. Deve permitir teste de disponibilidade de servidor web através do método TCP Half Open.
3.5.7.14. Deve permitir teste de disponibilidade de servidor web através do método TCP SSL.
3.5.7.15. Deve permitir teste de disponibilidade de servidor web através do método HTTP.
3.5.7.16. Deve permitir teste de disponibilidade de servidor web através do método HTTPS.
3.5.7.17. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar a URL exata a ser testada.
3.5.7.18. Nos testes de disponibilidade HTTP e HTTPS, permitir escolher entre os métodos HEAD, GET e POST.
3.5.7.19. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar o nome do campo HTTP "host" a ser testado.
3.5.7.20. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Host".
3.5.7.21. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "URL".
3.5.7.22. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Parâmetro HTTP".
3.5.7.23. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Referer".
3.5.7.24. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Endereço IP de Origem".
3.5.7.25. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Cabeçalho".
3.5.7.26. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Cookie".
3.5.7.27. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Valor de campo
3.5.7.28. do Certificado X509".
3.5.7.29. Deve implementar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados e requisições HTTP sejam respondidas diretamente pela solução.
3.5.7.30. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por endereço IP de origem.
3.5.7.31. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando parâmetros do header HTTP.
3.5.7.32. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada.
3.5.7.33. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por cookie – método cookie insert e cookie rewrite.
3.5.7.34. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por embedded cookie (cookie original mais porção randômica).
3.5.7.35. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Reescrita de Cookie.

3.5.7.36. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Cookie Persistente.

3.5.7.37. A solução ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em ASP Session ID.

3.5.7.38. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em PHP Session ID.

3.5.7.39. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em JSP Session ID.

3.5.7.40. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por sessão SSL.

3.5.7.41. A solução deve ser capaz de enviar código de erro 503 caso o helth-check dos servidores estiver desabilitado e/ou o servidor/serviço de retaguarda não estiver responsivo.

3.5.7.42. Deve suportar FWMARK (marcação de tráfego).

3.6. ITEM 06 – SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAF TIPO II

3.6.1. CARACTERÍSTICAS E FUNCIONALIDADES GERAIS

3.6.1.1. A solução deve ser entregue em appliance ou no formato de solução virtual, compatível com as plataformas VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, no caso de solução virtualizada a responsabilidade pela implantação de servidor/hardware com licenciamento necessário será da CONTRATADA, e o equipamento deve ser instalado no local indicado pela CONTRATANTE.

3.6.1.2. Poderá ser entregue em equipamento único ou com composição de equipamentos. para atender as funcionalidades exigidas.

3.6.1.3. A solução deverá ser fornecida com licenças para utilização durante a vigência contratual de 24 (vinte e quatro) meses, com as funcionalidades habilitadas de AV, IPS, WAF Security Service, IP Reputation, Sandbox, Credential Stuffing Defense Service.

3.6.2. Requisitos Mínimos de Performance

3.6.2.1. Deve possuir throughput mínimo para HTTP de 6 (seis) Gbps;

3.6.2.2. Deve suportar quantidade ilimitada de aplicações protegidas;

3.6.2.3. Deve suportar até 10 interfaces de rede;

3.6.2.4. Deve suportar até 16 vCPU;

3.6.3. Requisitos Mínimos de Funcionalidades

3.6.3.1. Todos os equipamentos que compõem a solução devem ser entregues com a última versão de software homologada e recomendada pelo fabricante.

3.6.3.2. Deve ser fornecida Solução Centralizada de Armazenamento de Logs e Relatórios, caso compatível poderá ser utilizada atual solução existente na PRODEB, Marca Fortinet, Modelo FAZ-3700G.

3.6.3.3. A solução proposta deve contemplar para a solução de armazenamento, análise de logs e relatoria o projeto de implantação, migração, garantia, capacitação da equipe local e suporte.

3.6.4. Funcionalidades de Rede

3.6.4.1. A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso), Passivo, ou "Sniffer"

3.6.4.2. (Offline) e Inline Transparente (Bridge).

3.6.4.3. A solução deve ser capaz de ser implementada com protocolo WCCP.

3.6.4.4. Suportar VLANs no padrão IEEE 802.1q.

3.6.4.5. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP) - IEEE 802.3ad.

3.6.4.6. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs).

3.6.4.7. A solução deve suportar roteamento por política (policy route).

3.6.5. Funcionalidades de Gerência

3.6.5.1. O sistema operacional / firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, e através de CLI (interface de linha de comando), acessando localmente, via porta de console, ou remotamente via SSH.

3.6.5.2. Deve possuir administração baseada em interface web HTTPS.

3.6.5.3. Possuir auto-complementação de comandos na CLI.

3.6.5.4. Possuir ajuda contextual na CLI.

3.6.5.5. A solução deve possuir Interface Gráfica com informações sobre o sistema Ex: (Informações do Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware).
3.6.5.6. Deve ser possível visualizar através da interface gráfica de gerência informações de licenças e assinaturas.
3.6.5.7. Deve prover, na interface de gerência, as seguintes informações do sistema para cada gateway: consumo de CPU e estatísticas das conexões.
3.6.5.8. Deve ser possível visualizar na interface de gerência as informações de consumo de memória.
3.6.5.9. Deve ser possível visualizar na interface de gerência ou CLI as informações de utilização de disco de log.
3.6.5.10. Deve possuir ferramenta, na interface gráfica de gerência (dashboard) que permita visualizar os últimos logs de ataque detectados/bloqueados.
3.6.5.11. Deve prover as seguintes informações, na interface de gráfica de gerência: estatísticas de throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema.
3.6.5.12. Possuir na interface gráfica estatísticas de conexões concorrentes e por segundo, de políticas de segurança do sistema.
3.6.5.13. Possuir um painel de visualização com informações das interfaces de rede do sistema.
3.6.5.14. A configuração de administração da solução deve possibilitar a utilização de perfis.
3.6.5.15. Deve ser possível executar e restaurar backup via interface Web (GUI).
3.6.5.16. Deve ter a opção para criptografar o backup.
3.6.5.17. Deve ser possível executar e restaurar backup utilizando-se um ou mais dos seguintes protocolos: FTP, SFTP ou TFTP,ou HTTPS
3.6.5.18. Deve ser possível instalar um firmware alternativo em disco e inicializá-lo manualmente em caso de falha do firmware principal.
3.6.5.19. Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3.
3.6.5.20. Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog.
3.6.5.21. A solução deve ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG.
3.6.5.22. Ter a capacidade de armazenar logs em appliance remoto.
3.6.5.23. A solução deve ter a capacidade de adicionar identificadores customizados nos registros syslog antes de envio, como hostname, atrelados a valores fixos ou variáveis.
3.6.5.24. A solução deve ter a capacidade de enviar alertas por e-mail de eventos baseados em severidades e/ou categorias.
3.6.5.25. A solução deve possuir dados analíticos contendo localização geográfica dos clientes web.
3.6.5.26. A solução deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem, o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (hits) e percentual de cada país de origem.
3.6.5.27. Deve ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário.
3.6.5.28. Deve ter suporte a RESTful API para gerenciamento de configurações.
3.6.5.29. Deve suportar todas as funcionalidades para comunicação HTTP/2
3.6.6. Funcionalidades de Autenticação
3.6.6.1. Os usuários devem ser capazes de autenticar através do cabeçalho de autorização HTTP / HTTPS.
3.6.6.2. Os usuários devem ser capazes de autenticar através de formulários HTML embutidos.
3.6.6.3. A solução deve ser capaz de autenticar usuários através de certificados digitais pessoais.
3.6.6.4. Deve possuir base local para armazenamento e autenticação contas de usuários.
3.6.6.5. A solução deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS.
3.6.6.6. Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM.
3.6.6.7. A solução deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação.
3.6.7. Funcionalidades de Web Application Firewall
3.6.7.1. 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.
3.6.7.2. Deve implementar recursos de Sandbox para análise de malware moderno;
3.6.7.3. 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.

3.6.7.4. Deve implementar proteção contra a lista de técnicas/ataques listados no OWASP 10 (Open Web Application security Project)
3.6.7.5. 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.
3.6.7.6. Ter a capacidade de criação de assinaturas de ataque customizáveis.
3.6.7.7. Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol.
3.6.7.8. Ter a capacidade de proteção para ataques do tipo Botnet.
3.6.7.9. Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST).
3.6.7.10. A solução deve possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta.
3.6.7.11. Deve suportar detecção a ataques de Clickjacking.
3.6.7.12. Deve suportar detecção a ataques de alteração de cookie.
3.6.7.13. Deve identificar e prevenir ataques do tipo Credit Card Theft.
3.6.7.14. Deve identificar e prevenir ataque Cross Site Request Forgery (CSRF).
3.6.7.15. A solução deve possuir funcionalidade de proteção positiva contra ataques como cross site scripting (XSS).
3.6.7.16. Deve possuir proteção contra ataques de Denial of Service (DoS).
3.6.7.17. Deve possuir a capacidade de proteção para ataques do tipo HTTP header overflow.
3.6.7.18. Deve possuir a capacidade de proteção para ataques do tipo Local File inclusion (FLI).
3.6.7.19. Deve possuir a capacidade de proteção para ataques do tipo Man-in-the-middle (MITM).
3.6.7.20. Deve possuir a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI).
3.6.7.21. Deve possuir a capacidade de proteção para ataques do tipo Server Information Leakage.
3.6.7.22. Deve possuir proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection).
3.6.7.23. Deve possuir a capacidade de proteção para ataques do tipo Malformed XML.
3.6.7.24. Deve Identificar e prevenir ataques do tipo Low-rate DoS.
3.6.7.25. Deve possuir prevenção contra Slow POST attack.
3.6.7.26. Deve proteger contra ataques Slowloris.
3.6.7.27. Deve possuir a capacidade de proteção para ataques do tipo SYN flood.
3.6.7.28. Deve possuir a capacidade de proteção para ataques do tipo Forms Tampering.
3.6.7.29. A solução deve possuir funcionalidade de proteção positiva contra ataques de manipulação de campo escondido.
3.6.7.30. Deve possuir a capacidade de proteção para ataques do tipo Directory Traversal.
3.6.7.31. Deve possuir a capacidade de proteção do tipo Access Rate Control.
3.6.7.32. 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.
3.6.7.33. Deve permitir configurar regras de bloqueio a métodos HTTP indesejados.
3.6.7.34. Deve permitir que sejam configuradas regras de limite de upload por tamanho de arquivo.
3.6.7.35. 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.
3.6.7.36. Deve permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem.
3.6.7.37. Deve permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.
3.6.7.38. Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation.
3.6.7.39. Deve possuir a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP.
3.6.7.40. Deve possuir a funcionalidade de proteger o website contra ações de desfiguração (defacement), com restauração automática e rápida do site caso ocorra à falha.
3.6.7.41. Deve possuir a funcionalidade de antivírus para inspeção de tráfego e arquivos.
3.6.7.42. Deve possuir a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não-conformidade.
3.6.7.43. 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.

3.6.7.44. A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego.
3.6.7.45. Deve para SSL/TLS offload suportar no mínimo TLS 1.0, 1.1, 1.2 e 1.3.
3.6.7.46. A solução deve ter a capacidade de armazenar certificados digitais de CA's.
3.6.7.47. A solução deve ser capaz de gerar CSR para ser assinado por uma CA.
3.6.7.48. A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL).
3.6.7.49. 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.
3.6.7.50. 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.
3.6.7.51. A solução deve ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores.
3.6.7.52. 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.
3.6.7.53. 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).
3.6.7.54. A solução deve ter a capacidade de definir restrições a métodos HTTP.
3.6.7.55. A solução deve ter a capacidade de proteger contra a detecção de campos ocultos.
3.6.7.56. Deve permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares.
3.6.7.57. 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,
3.6.7.58. Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros.
3.6.7.59. A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML.
3.6.7.60. A solução deve permitir a exclusão de URLs na análise de vulnerabilidades.
3.6.7.61. Deve ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente.
3.6.7.62. Deve suportar redireção e reescrita de requisições e respostas HTTP.
3.6.7.63. Deve permitir redirecionar requisições HTTP para HTTPS.
3.6.7.64. Deve permitir reescrever a linha URL no cabeçalho de uma requisição HTTP.
3.6.7.65. Deve permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP.
3.6.7.66. Deve permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP.
3.6.7.67. Deve permitir redirecionar requisições para outro web site.
3.6.7.68. Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP.
3.6.7.69. Deve permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web.
3.6.7.70. Deve permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor web.
3.6.7.71. Deve permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso.
3.6.7.72. 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).
3.6.7.73. 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.
3.6.7.74. Possuir capacidade de caching para aceleração web.
3.6.7.75. Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.
3.6.7.76. Deve suportar no mínimo 500 regras de reescrita URL distintas
3.6.7.77. Deve suportar no mínimo 250 políticas de assinatura distintas
3.6.7.78. Deve suportar no mínimo 500 grupos ou pools de servidores, e cada pool deve suportar no mínimo 1000 membros
3.6.7.79. Deve suportar no mínimo 1000 IPs virtuais configurados e ativos simultaneamente
3.6.7.80. Deve ser capaz de restringir acesso quando as requisições não tiverem um cabeçalho HTTP específico pré-configurado.

3.6.7.81. Deve ser capaz de limitar o número de usuários/origens simultâneos acessando a mesma conta/sessão/login.

3.6.7.82. 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.

3.6.7.83. Deve ser capaz de adicionar múltiplos servidores ADFS em um pool de servidores

3.6.7.84. 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.

3.6.8. Outras funcionalidades

3.6.8.1. A solução deve incluir funcionalidade de balanceamento de carga entre servidores web.

3.6.8.2. Deve possuir a habilidade de configurar portas não-padrão para aplicação web HTTP e HTTPS.

3.6.8.3. Deve possuir a capacidade de balancear/distribuir tráfego e rotear o conteúdo através de vários servidores web.

3.6.8.4. A solução deve permitir criar grupos de servidores (Server Farm / Pool) para distribuir as conexões dos usuários.

3.6.8.5. Deve suportar algoritmo Round Robin para balanceamento de carga de servidores.

3.6.8.6. Deve suportar algoritmo Weighted Round Robin para balanceamento de carga de servidores.

3.6.8.7. Deve suportar algoritmo Least Connections para balanceamento de carga de servidores.

3.6.8.8. A solução deve ser capaz de criar servidores virtuais que definem a interface de rede/bridge e endereço IP por onde o tráfego destinado ao Server Pool é recebido.

3.6.8.9. Os servidores virtuais devem entregar o tráfego à um único servidor web e também possuir a opção de distribuir as sessões/conexões entre os servidores web do Server Pool.

3.6.8.10. Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do Server Pool.

3.6.8.11. Deve permitir teste de disponibilidade de servidor web através do método TCP.

3.6.8.12. Deve permitir teste de disponibilidade de servidor web através do método ICMP ECHO_REQUEST (ping).

3.6.8.13. Deve permitir teste de disponibilidade de servidor web através do método TCP Half Open.

3.6.8.14. Deve permitir teste de disponibilidade de servidor web através do método TCP SSL.

3.6.8.15. Deve permitir teste de disponibilidade de servidor web através do método HTTP.

3.6.8.16. Deve permitir teste de disponibilidade de servidor web através do método HTTPS.

3.6.8.17. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar a URL exata a ser testada.

3.6.8.18. Nos testes de disponibilidade HTTP e HTTPS, permitir escolher entre os métodos HEAD, GET e POST.

3.6.8.19. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar o nome do campo HTTP "host" a ser testado.

3.6.8.20. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Host".

3.6.8.21. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "URL".

3.6.8.22. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Parâmetro HTTP".

3.6.8.23. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Referer".

3.6.8.24. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Endereço IP de Origem".

3.6.8.25. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Cabeçalho".

3.6.8.26. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Cookie".

3.6.8.27. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Valor de campo

3.6.8.28. do Certificado X509".

3.6.8.29. Deve implementar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados e requisições HTTP sejam respondidas diretamente pela solução.

3.6.8.30. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por endereço IP de origem.

3.6.8.31. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando parâmetros do header HTTP.
3.6.8.32. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada.
3.6.8.33. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por cookie – método cookie insert e cookie rewrite.
3.6.8.34. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por embedded cookie (cookie original mais porção randômica).
3.6.8.35. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Reescrita de Cookie.
3.6.8.36. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Cookie Persistente.
3.6.8.37. A solução ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em ASP Session ID.
3.6.8.38. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em PHP Session ID.
3.6.8.39. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em JSP Session ID.
3.6.8.40. A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por sessão SSL.
3.6.8.41. A solução deve ser capaz de enviar código de erro 503 caso o helth-check dos servidores estiver desabilitado e/ou o servidor/serviço de retaguarda não estiver responsivo.
3.6.8.42. Deve suportar FWMARK (marcação de tráfego).

3.7. ITEM 07 – SOLUÇÃO DE SEGURANÇA DECOY/HONEYPOT

3.7.1. Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização: VMWare vSphere ESXi 5.1, 5.5 ou 6.0 and later, KVM, Hyper-V, AWS. AZURE, GCP. No caso de solução virtualizada a responsabilidade pelo fornecimento de servidor/hardware com licenciamento necessário será da CONTRATADA, e o equipamento deve ser instalado no local indicado pela CONTRATANTE
3.7.2. Deve possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 24 (vinte e quatro) meses.
3.7.3. Poderá ser entregue em equipamento único ou com composição de equipamentos para atender as funcionalidades exigidas.
3.7.4. Deve suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções
3.7.5. Deve ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.
3.7.6. Deve ser fornecida Solução Centralizada de Armazenamento de Logs e Relatórios, caso compatível poderá ser utilizada atual solução existente na PRODEB, Marca Fortinet, Modelo FAZ-3700G.
3.7.7. Deve suportar ter a capacidade mínima de 18 VM de honeypot;
3.7.8. Deve suportar no mínimo 120 VLAN's e estar licenciado para no mínimo 05 VLAN's;
3.7.9. Deve possuir 02 (dois) licenciamento incluso de Windows 7 ou Windows 10.
3.7.10. Deve possuir licenciamento pelo período de 24 (vinte e quatro) meses para as funcionalidades de Deception Decoys, AV, IPS, e Web Filtering;
3.7.11. Deve suportar a seguinte combinação:
3.7.11.1. Windows 7, Windows 10, Windows 10 (customizable BYOL), Windows Server 2016 and 2019 ou superior
3.7.11.2. Linux, VPN Server
3.7.11.3. Medical (PACS, Infusion pump), ERP
3.7.11.4. IoT, SAP and/or SCADA
3.7.12. Deve suportar os seguintes serviços:
3.7.12.1. SSL VPN, 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
3.7.13. Deve possuir as certificações: FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

3.7.14. 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.
3.7.15. Deve ser capaz de monitorar as ações de atacantes que tentem violar as máquinas virtuais.
3.7.16. Deve analisar as ações dos invasores ao tentarem invadir as máquinas virtuais.
3.7.17. Deve ser capaz de simular serviços, aplicativos ou usuários nas máquinas virtuais a fim de simular um ambiente corporativo real.
3.7.18. Deve possibilitar a instalação de pacote ou script em endpoits reais que simulem interação com os serviços das máquinas virtuais a fim de influenciar o comportamento dos atacantes aumentando a superfície de engano.
3.7.19. O administrador deve ser capaz de monitorar ataques através de incidentes, lista de ataques e por representação vistual da rede mostrando endpoints, maquinas virtuais do dispositivo e ataques em andamento.
3.7.20. 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.
3.7.21. Deve suportar a criação de perfis de administrador para controlar os privilégios de acesso do aos recursos do sistema. Ao criar uma conta de administrador deve ser atribuído um perfil à conta;
3.7.22. 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;
3.7.23. Deve suportar a autenticação remota de administradores usando servidores RADIUS e LDAP;
3.7.24. Deve ser capaz de ser implantado em redes do tipo offline ou air-gapped
3.7.25. Deve permitir inserir a licença de uso do equipamento mesmo em redes do tipo offline ou air-gapped
3.7.26. Deve ser capaz de atualizar o firmware mesmo em redes do tipo offline ou air-gapped;
3.7.27. Deve ser capaz de atualizar o módulo de segurança mesmo em redes do tipo offline ou air-gapped;
3.7.28. Deve ser capaz de armazenar Log no próprio equipamento ou integrar com um servidor remoto de armazenamento de log;
3.7.29. Deve suportar servidor de log remoto do tipo syslog e CEF.
3.7.30. Deve possuir dashboard que mostre informações dos seguintes itens:
3.7.30.1. Informações do sistema como: Hostname, versão do firmware e usuário conectado no momento;
3.7.30.2. Número de incidente e eventos com sueus níveis de severidade por intervalo de tempo;
3.7.30.3. Número de decoy implementado;
3.7.30.4. Performance de CPU e RAM;
3.7.30.5. Informação de uso de disco;
3.7.30.6. Widget de Top attack;
3.7.31. Deve ser capaz de customizar o dashboard;
3.7.32. Deve ser capaz de atualizar o firmware via interface gráfica;
3.7.33. Deve ser capaz de realizar o backup e restore via interface gráfica;
3.7.34. Deve ser capaz de configurar rotas (camada 3 OSI);
3.7.35. Deve suportar configuração de cliente DNS;
3.7.36. Deve suportar configuração de IPv4 e IPv6;
3.7.37. Deve ser capaz de criar diferentes perfis de conta de administrador do sistema;
3.7.38. Deve ser capaz de integrar com servidor LDAP e Radius;
3.7.39. Deve suportar a importação de certificados CA;
3.7.40. Deve suportar a confguração de cliete de e-mail para envio de alertas;
3.7.41. Deve ser capaz de escolher o nível de severidade do alerta que será enviado;
3.7.42. Deve suportar SNMP V1, V2 e V3;
3.7.43. Deve suportar conexão com a base de dados do fabricante para atualizar informações de segurança;
3.7.44. Deve suportar integração com sistema de detecção de malware
3.7.45. Deve suportar integração com SandBox
3.7.46. Deve suportar integração com NGFW do mesmo fabricante ou de terceiros;
3.7.47. Quando integrado com solução de NGFW deve permitir:
3.7.47.1. Quarentenar dispositivos;
3.7.47.2. Exibir o status de IP bloqueado;
3.7.47.3. Exportar arquivo IOC no formato CSV ou STIX;
3.7.47.4. Mitigar e isolar de forma automática endpoint infectado para previnir ataques ou movimentação lateral na rede;

3.7.48. 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;
3.7.49. Deve ser capaz de gerar relatórios em PDF ou CSV;
3.7.50. Deve ser capaz de listar os ataques detectados com as informações de severidade, data e hora, informação do IP do atacante;
3.7.51. Deve ser capaz de montar uma representação da rede em forma de mapa contendo informação do endpoint, decoy e ataque;
3.7.52. Deve ser capaz de classificar o nível de risco dos incidentes e eventos;
3.7.53. Deve ser capaz de informar a quantidade de eventos e incidentes que ocorreram em uma faixa de tempo;
3.7.54. Deve ser capaz de listar pelo menos o top 5 atacantes;
3.7.55. Deve ser capaz de listar o número de incidente por serviço de forma gráfica;
3.7.56. 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;
3.7.57. Deve ser capaz de implementar decoy customizado (custom image);
3.7.58. Deve suportar importação de imagem ISO;
3.7.59. Deve ser capaz de customizar o recuso de CPU, Memória e Armazenamento da VM-decoy;

3.8. ITEM 08 – SOLUÇAO DE SEGURANÇA DE EMAIL

3.8.1. Requisitos Gerais

3.8.1.1. A solução deve ser entregue em appliance ou no formato de solução virtual, compatível com as plataformas VMware, Microsoft Hyper-V e KVM, no caso de solução virtualizada a responsabilidade pelo fornecimento de servidor/hardware com licenciamento necessário será da CONTRATADA, e o equipamento deve ser instalado no local indicado pela CONTRATANTE;
3.8.1.2. Deve possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 24 (vinte e quatro) meses.
3.8.1.3. Deve ser fornecida Solução Centralizada de Armazenamento de Logs e Relatórios, caso compatível poderá ser utilizado atual solução existente na PRODEB, Marca Fortinet, Modelo FAZ-3700G.
3.8.1.4. Deve suportar o roteamento de, no mínimo, 3.000.000 (três milhões) mensagens por hora;
3.8.1.5. Suportar o roteamento de, no mínimo, 2.500.000 (dois milhões e quinhentos mil) mensagens por hora com a análise de anti-spam;
3.8.1.6. Suportar o roteamento de, no mínimo, 2.000.000 (dois milhões) mensagens por hora com a análise de anti-spam e anti-vírus;
3.8.1.7. Permitir a configuração de, no mínimo, 2.000 (dois mil) domínios;
3.8.1.8. Permitir a configuração de, no mínimo, 40.000 (quarenta mil) mailboxes quando operando em modo gateway.

3.8.2. Funcionalidades Gerais

3.8.2.1. A solução deve possuir e estar licenciada com funcionalidades de anti-spam, anti-vírus, anti-spyware e anti-phishing. deve ser capaz de realizar a inspeção de correio da Internet de entrada e saída.
3.8.2.2. Deve permitir integração com o Microsoft 365 através de API;
3.8.2.3. Deve ter a opção de remover ou neutralizar conteúdos potencialmente maliciosos e reconstruí- lo mais tarde. Por exemplo, em arquivos como o MSOffice e o pdf que possuem macros, java ou HTML com URLs mal-intencionados;
3.8.2.4. Deve possuir um assistente (wizard) para o provisionamento fácil e rápido de configurações básicas e domínios para proteção.
3.8.2.5. Deve se conectar em tempo real com a base de dados do fabricante para baixar atualizações anti-spam.
3.8.2.6. Deve oferecer proteção contra-ataques de negação de serviço como, por exemplo, Mail Bomb.
3.8.2.7. Deve permitir a criação de perfis de configuração de forma granular, onde, para cada perfil, poderá adicionar configurações específicas de funcionalidades, como: anti-spam, anti-vírus, autenticação, dentre outros.
3.8.2.8. Deve ser capaz de entregar o correio baseado em usuários existentes em uma base LDAP.
3.8.2.9. Deve suportar quarentena por usuário, possibilitando que cada usuário possa administrar sua própria quarentena, removendo mensagens ou liberando as que não são spam, diminuindo a responsabilidade do administrador e também a possibilidade de bloqueio de e-mails legítimos. A quarentena deve ser acessada através de página Web e POP3.
3.8.2.10. Deve ser capaz de agendar o envio de relatórios de quarentena.

3.8.2.11. Deve ser capaz de realizar o armazenamento de e-mails (archiving) baseado nas políticas de envio e recepção, com suporte também a armazenamento remoto.
3.8.2.12. Deve ser capaz de manter filas de correio (queue) em caso de falha na conexão de saída, atrasos ou erros de entrega.
3.8.2.13. Deve ser capaz de manter listas de reputação do remetente com base em: quantidade de vírus enviados, quantidade de e-mails considerados spams e quantidade de destinatários equivocados.
3.8.2.14. Deve ter a capacidade de avaliar, reter e/ou bloquear e-mails que têm ameaças avançadas, como dia-zero, através da análise com sandboxing.
3.8.2.15. Deve ser capaz de filtrar anexos e conteúdo de e-mails.
3.8.2.16. Deve ser capaz de realizar uma inspeção profunda de cabeçalhos de e-mail. deve ser capaz de realizar análise bayesiana para determinar se um e-mail é spam.
3.8.2.17. Deve ser capaz de filtrar e-mails baseados nos URI's (Uniform Resource Identifier) contidos no corpo da mensagem.
3.8.2.18. Deve ser capaz de realizar análise de imagem e documentos PDF para a procura de spam.
3.8.2.19. Deve suportar direcionamento em IPv4 e IPv6.
3.8.2.20. Deve suportar greylist para contas de e-mail em IPv4 e IPv6. deve ser capaz de detectar endereços IP forjados (Forged IP).
3.8.2.21. Deve ser capaz de funcionar como gateway, atuando como MTA (Mail Transfer Agent). deve suportar Sender Policy Framework (SPF).
3.8.2.22. Deve suportar Domain Keys Identified Mail (DKIM).
3.8.2.23. Deve suportar Domain Based Message Authentication (DMARC).
3.8.2.24. Deve ser capaz de atrasar o envio de e-mail de grandes dimensões para os horários que são de menos carga.
3.8.2.25. Deve ser capaz de definir o encaminhamento de correio (relay) para um IP específico baseado no IP de origem da mensagem.
3.8.2.26. Deve permitir o armazenamento de e-mails e quarentena localmente ou em servidor remoto.
3.8.2.27. Deve permitir sua configuração através de interface para acesso à Web (HTTP, HTTPS).
3.8.2.28. Deve ser capaz de permitir a criação de administradores exclusivos para administração e configuração da solução por domínio, sendo também possível restringir o acesso por endereço IP e máscara de rede de origem.
3.8.2.29. Deve ser capaz de fornecer, pelo menos 02 (dois) níveis de acesso de gestão:
3.8.2.30. Leitura/Gravação (Read/Write) ou Somente Leitura (Read Only).
3.8.2.31. Deve ser capaz de armazenar logs e eventos localmente e também enviá-los para servidores remotos (Syslog).
3.8.2.32. Deve permitir o relato de atividades, analisando os arquivos de eventos (logs) e apresentá-los na tabela ou formato gráfico.
3.8.2.33. Quando a solução estiver implementada em alta disponibilidade, deve ser capaz de monitorar o status do link.
3.8.2.34. Quando a solução estiver implementada em alta disponibilidade, deve suportar o failover de rede.
3.8.2.35. Quando a solução estiver implementada em alta disponibilidade, deve suportar o modo ativo/passivo.

3.8.3. Funcionalidades de DLP

3.8.3.1. A funcionalidade de DLP deve permitir especificar a informação a ser detectada como palavras, frases e expressões regulares.
3.8.3.2. Deve possuir uma lista predefinida de tipos de informações, como números de cartão de crédito e outros.
3.8.3.3. Deve permitir a criação e armazenamento de impressões digitais (fingerprint) de documentos.
3.8.3.4. Deve permitir a criação de filtros por arquivo.
3.8.3.5. Deve permitir a geração e armazenamento de impressões digitais (fingerprint) de anexos em e- mail.

3.8.4. Funcionalidades de IBE

3.8.4.1. A solução deve suportar criptografia das mensagens baseada em identidade (Identity Based Encryption IBE) para que o destinatário não requeira uma PSK ou certificado instalado anteriormente para a descriptografia.
3.8.4.2. Deve possuir licenças Email Data Loss Prevention, URL Click Protection e Cloud Sandboxing;
3.8.4.3. A criptografia de mensagens com IBE deve suportar tanto o método push, quanto o método pull, em que a mensagem criptografada é armazenada na plataforma de e-mail para acesso remoto autenticado ou ser enviada como anexo para o destinatário.

3.8.4.4. Em ambos métodos da criptografia IBE, deve ter um registro do usuário do destino na plataforma de e-mail, de modo que, para ver as mensagens criptografadas, um processo de autenticação seja necessário.

3.8.5. Suporte a RFC's

3.8.5.1. A solução deve suportar as seguintes RFC's (Request For Comments):

3.8.5.2. Criptografia SMTPS e SMTP over TLS;

3.8.5.3. RFC 1985 (SMTP Service Extension for Remote Message Queue Starting); RFC 2034 (SMTP Service Extension for Returning Enhanced Error Codes); RFC 3207 (SMTP Service Extension for Secure SMTP over TLS);

3.8.5.4. RFC 3461 (SMTP Service Extension for Delivery Status Notifications DSNs); RFC 3463 (Enhanced Mail System Status Codes);

3.8.5.5. RFC 3464 (Extensible Message Format for Delivery Status Notifications); RFC 4954 (SMTP Service Extension for Authentication);

3.8.5.6. RFC 5321 (SMTP);

3.8.5.7. RFC 6376 (DomainKeys Identified Mail (DKIM) Signatures);

3.8.5.8. RFC 6522 (Multipart/Report Content Type for the Reporting of Mail System Administrative Messages);

3.8.5.9. RFC 7208 (Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail);

3.8.5.10. RFC 2221 (Login Referrals);

3.8.5.11. RFC 2342 (IMAP4 Namespace);

3.8.5.12. RFC 2683 (IMAP4 Implementation Recommendations); RFC 2971 (IMAP4 ID Extension);

3.8.5.13. RFC 3348 (IMAP4 Child Mailbox Extension); RFC 3501 (IMAP4 rev1);

3.8.5.14. RFC 3502 (IMAP Multiappend Extension);

3.8.5.15. RFC 3516 (IMAP4 Binary Content Extension); RFC 3691 (Unselect Command);

3.8.5.16. RFC 4315 (UIDPLUS Extension); RFC 4469 (Catenate Extension);

3.8.5.17. RFC 4731 (Extension to SEARCH Command for Controlling What Kind of Information Is Returned);

3.8.5.18. RFC 4959 (Extension for Simple Authentication and Security Layer (SASL) Initial Client Response);

3.8.5.19. RFC 5032 (WITHIN Search Extension); RFC 5161 (Enable Extension);

3.8.5.20. RFC 5182 (Extension for Referencing the Last SEARCH Result); RFC 5255 (IMAP Internationalization);

3.8.5.21. RFC 5256 (Sort and Thread Extensions); RFC 5258 (List Command Extensions); RFC 5267 (Contexts for IMAP4);

3.8.5.22. RFC 5819 (Extension for Returning STATUS Information in Extended LIST); RFC 6154 (LIST Extension for Special-Use Mailboxes);

3.8.5.23. RFC 6851 (MOVE Extension);

3.8.5.24. RFC 7162 (IMAP Extensions:Quick Flag Changes Resynchronization (CONDSTOR) and Quick Mailbox Resynchronization (QRESYNC));

3.8.5.25. RFC 1939 (POP3);

3.8.5.26. RFC 2449 (POP3 Extension Mechanism);

3.8.5.27. RFC 1155 (Structure and Identification of Management Information for TCP/IP-based Interface);

3.8.5.28. RFC 1157 (SNMP v1); RFC 1213 (MIB 2);

3.8.5.29. RFC 2578 (Structure of Management Information Version 2); RFC 2579 (Textual Conventions for SMIv2);

3.8.5.30. RFC 2595 (Using TLS with IMAP, POP3 and ACAP); RFC 3410 (SNMP v3);

3.8.5.31. RFC 3416 (SNMP v2).

3.9. ITEM 09 – SERVIÇOS PROFISSIONAIS DE MONITORAMENTO E SEGURANÇA DO DATACENTER DA PRODEB

3.9.1. CARACTERISTICAS GERAIS

3.9.1.1. A CONTRATADA deve prestar durante a vigência contratual de 24 (vinte e quatro) meses, serviços profissionais, especializados e multidisciplinares para o monitoramentoe a proteção do ambiente de datacenter da PRODEB, incluindo Gestão de Vulnerabilidades, Gestão de Incidentes, Monitoramento e Visibilidade de ataques Cibernéticos, Operação e Atendimento de Requisições, Testes de Invasão, Simulação de ataques relacionados à Segurança Digital;

3.9.1.2. Os serviços acima devem considerar como escopo inicial as soluções e produtos de segurança descritos no ANEXO III – SOLUÇÕES DE SEGURANÇA e deve realizar, durante a vigência do contrato, ações proativas voltadas para a segurança do parque computacional da PRODEB a fim de e mantê-lo estável, disponível e integro;

3.9.1.3. As soluções de segurança a serem contratadas e que constam nos itens 06, 07 e 08 também farão parte do escopo deste serviço;

3.9.1.4. No prazo de até 30 (trinta) dias após a emissão da Ordem de Serviço, a CONTRATADA deverá realizar avaliação completa do ambiente do CONTRATANTE com o objetivo identificar lacunas ou oportunidades de melhoria (Gap Analysis) com o objetivo de avaliar a maturidade dos controles de segurança do CONTRATANTE;

3.9.1.4.1. A análise dos controles de segurança deverá ser realizada obedecendo o framework de segurança MITRE ATT&CK que utiliza base global de conhecimento das táticas, técnicas e procedimentos (TTP's) utilizados por atacantes para avaliar a efetividade dos controles de segurança;

3.9.1.4.2. A análise deverá ser conduzida por profissional com certificação CISSP – Certified Information Systems Security, que será responsável pela apresentação dos resultados da análise ao gestor, fiscais do contrato e gestores da PRODEB;

3.9.1.4.3. Deverá fornecer os resultados da análise para a equipe técnica da CONTRATANTE;

3.9.2. PRINCIPAISATIVIDADES A SEREM EXECUTADAS DE FORMA CONTÍNUA PELA CONTRATADA:

3.9.2.1. Interagir com a equipe de Segurança da PRODEB de forma contínua para otimização das ações de proteção do ambiente, definição de processos, procedimentos operacionais e instruções de trabalho;

3.9.2.2. Acompanhar a execução dos serviços para o cumprimento dos níveis de serviço estabelecidos;

3.9.2.3. Priorizar os atendimentos críticos, conforme definição do CONTRATANTE;

3.9.2.4. Monitorar permanente e avaliar criticamente os produtos e serviços de segurança do CONTRATANTE;

3.9.2.5. Traçar curvas de comportamento, definir a volumetria média de acessos e identificar comportamentos não usuais, visando an tecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços;

3.9.2.6. Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;

3.9.2.7. Reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de TI do CONTRATANTE;

3.9.2.8. Atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TI.

3.9.2.9. Prover os fiscais do contrato com os relatórios técnicos e gerenciais suficientes para a comprovação dos serviços realizados;

3.9.2.10. Supervisionar sua equipe na execução dos serviços;

3.9.2.11. Elaborar e propor plano de execução dos serviços;

3.9.2.12. Organizar a alocação de turnos e de profissionais de sua equipe;

3.9.2.13. Definir plano de treinamento inicial e contínuo dos profissionais que executam os serviços;

3.9.2.14. Executar outros serviços correlatos à supervisão dos profissionais na execução dos Serviços;

3.9.2.15. Orientar a atuação da equipe técnica em situações críticas de trabalho, bem como interagir com a Equipe de Segurança da PRODEB;

3.9.2.16. Fornecer sugestões e auxiliar na construção e manut enção contínua, com o apoio e aprovação da CONTRATANTE, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;

3.9.2.17. Receber as demandas dos serviços relativas à área de segurança da informação e providenciar a execução e alocação de recursos de trabalho;

3.9.2.18. Consolidar os relatórios de atividades mensais (mês calendário), referente aos Serviços, provendo informações gerenciais ao CONTRATANTE;

3.9.2.19. Supervisionar sua equipe de profissionais na execução das ações conjuntas com as áreas de segurança e infraestrutura da CONTRATANTE, cumprindo a política de segurança da informação da CONTRATANTE e aplicando as melhores práticas de segurança;

3.9.2.20. Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades;

3.9.2.21. Elaborar mensalmente relatórios de desempenho, auditoria e operação dos ativos sob sua administração;

3.9.2.22. Implantar as melhorias solicitadas pela CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TI;

3.9.2.23. Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do CONTRATANTE na gestão de segurança da informação;

3.9.2.24. Aplicar os seguintes processos do ITIL: Gerenciamento de Incidente, Cumprimento de Requisição, Gerenciamento de Problema, Gerenciamento da Configuração e de Ativo de Serviço, Gerenciamento de Mudança, Gerenciamento de Liberação e Implantação, Gerenciamento da Disponibilidade, Gerenciamento do Conhecimento, Gerenciamento de Níveis de Serviço, Gerenciamento do Catálogo de Serviço.

3.9.2.25. Manter atualizado o Configuration Management Database (CMDB) na ferramenta de Gerenciamento de a ser disponibilizada pela CONTRATANTE;

3.9.2.26. Consolidar as sugestões de melhoria;

3.9.2.27. Receber as diretrizes relacionadas à área de Segurança da Informação e providenciar a execução e alocação de recursos de trabalho;

3.9.2.28. Apoiar e participar na implementação dos processos bem como na mensuração dos indicadores de objetivos instituídos pelo CONTRATANTE;

3.9.2.29. Realizar as atividades em estrita observância na Política de Segurança da Informação e demais normas estipuladas pelo CONTRATANTE;

3.9.2.30. Gerar e consolidar os relatórios de ataques, atualização de ativos, atualização de softwares (aplicação de patches e fix) dos produtos e serviços de segurança do CONTRATANTE constantes no ANEXO III – SOLUÇÕES DE SEGURANÇA, para apresentação ao CONTRATANTE, constando as medidas tomadas e sugestões;

3.9.2.31. Consolidar em manuais e scripts todos os serviços e soluções adotadas sejam eles novos ou já implantados no CONTRATANTE;

3.9.2.32. Auxiliar na elaboração dos procedimentos e metodologias, e verificar e reportar o cumprimento dos mesmos pelas demais áreas de TI;

3.9.2.33. Apoiar o CONTRATANTE na análise e definição das regras de uso dos recursos computacionais do CONTRATANTE;

3.9.2.34. Implantar as melhorias solicitadas pelas equipes técnicas da CONTRATANTE através de chamamos;

3.9.2.35. Monitorar e propor soluções aos projetos/atividades em andamento otimizando-os quanto aos requisitos de Segurança da Informação;

3.9.2.36. Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de sistemas e administração de dados, a fim de prover soluções pa ra projetos/atividades em andamento;

3.9.2.37. Participar, quando solicitado, da implantação de projetos/soluções, substituição e atualização de soluções destinadas à Segurança da Infraestrutura de rede;

3.9.2.38. Realizar análise de tentativas de invasão a sistemas e equipamentos gerenciados pela CONTRATADA;

3.9.2.39. Monitorar e analisar os logs dos serviços de segurança (equipamentos, sistemas operacionais de servidores e clientes, conexões, programas utilizados etc.), propondo ações corretivas e de melhorias;

3.9.2.40. Execução de mudanças de configuração nos ativos sob sua administração;

3.9.2.41. Execução das atividades relativas aos normativos e governança do CONTRATANTE naquilo que for relativo à sua área de atuação;

3.9.2.42. Os serviços devem ser capazes de garantir a melhor utilização possível dos recursos de segurança existentes na empresa, bem como responder de forma efetiva a eventuais incidentes de segurança.

3.9.2.43. Os serviços devem incluir, mas não se limitarão a:

3.9.2.43.1. Gerenciamento de Soluções de Segurança Existentes: Gerenciamento de todas as soluções de segurança atualmente implementadas na PRODEB. Isso inclui a operacionalização, atualização e otimização dessas soluções para garantir que elas continuem a oferecer o mais alto nível de proteção, operando de acordo com as melhores práticas dos respectivos fabricantes.

3.9.2.43.2. Monitoramento de Segurança: Monitoramento contínuo do ambiente de datacenter para detectar e responder a qualquer atividade suspeita ou maliciosa. Isso inclui o uso de ferramentas avançadas de detecção de intrusões e sistemas de prevenção.

3.9.2.43.3. Gestão de Vulnerabilidades: Identificação e mitigação de vulnerabilidades no ambiente de datacenter. Isso inclui a realização de avaliações de vulnerabilidade.

3.9.2.43.4. Simulação de Violação e Ataque: Implementação de simulações de violação e ataque para testar a eficácia das medidas de segurança existentes e identificar áreas de melhoria. Isso ajudará a organização a entender como os atacantes podem tentar violar suas defesas e permitirá que a PRODEB tome medidas proativas para fortalecer sua segurança.

3.9.2.43.5. Gestão de Incidentes de Segurança: Resposta rápida e eficaz a incidentes de segurança para minimizar o impacto e garantir a recuperação rápida do sistema.

3.9.2.43.6. Segurança Operacional: Implementação de controles de acesso robustos para garantir que apenas indivíduos autorizados tenham acesso ao ambiente de datacenter. Todas as operações realizadas no ambiente operacional da PRODEB, seja local ou remotamente, devem ser gravadas e passíveis de auditoria.

3.9.2.43.7. Automação e Integração de Segurança: Implementação de automação e integração entre as diferentes soluções de segurança para otimizar a resposta a incidentes. Isso permitirá uma resposta mais rápida e eficaz a incidentes de segurança, minimizando o impacto potencial e melhorando a eficiência operacional;

3.9.2.43.8. Operacionalização e atendimento de mudanças e requisições: Realizar a operação das soluções de segurança gerenciadas a partir do atendimento de solicitações de mudança e requisições.

3.9.2.43.9. Todos os profissionais envolvidos e alocados para a prestação dos serviços, deverão ter vínculo formal com a empresa CONTRATADA.

3.9.3. AMBIENTE DA CONTRATANTE PRODEB

3.9.3.1. O ambiente de DataCenter da PRODEB é formado pelos seguintes dispositivos (servidores, switches, etc. etc.) que deverão ser protegidos pelos serviços;

3.9.3.2. As soluções de segurança instaladas no ambiente de segurança atual da PRODEB estão listadas no ANEXO III – SOLUÇÕES DE SEGURANÇA INSTALADAS NA PRODEB:

3.9.3.3. Todas fazem parte do escopo dos serviços de gerenciamento, operação, atendimento a requisições, monitoramento, resposta a incidentes, integração e automação a serem contratados e devem ser operadas pela CONTRATADA.

3.9.3.4. Outras soluções, necessárias ao cumprimento dos requisitos de serviço elencados neste Termo de Referência, e que não façam parte da tabela acima, deverão ser fornecidas pela CONTRATADA, sem ônus adicional para a PRODEB, em quantidade suficiente para o escopo do ambiente de DataCenter da PRODEB.

3.9.3.5. As soluções a serem utilizadas na prestação dos serviços aqui elencados, que forem de responsabilidade da CONTRATADA, deverão atender a todos os requisitos de funcionalidades de serviço descritos nas especificações técnicas deste termo de referência.

3.9.4. ESCOPO DOS SERVIÇOS DE SUPORTE E MONITORAMENTO

3.9.4.1. O fornecedor deverá fornecer um serviço de suporte, gerenciamento e monitoramento de todas as soluções de segurança atualmente existentes na PRODEB. Este serviço deve incluir a operacionalização, atualização e otimização dessas soluções para garantir que elas continuem a oferecer o mais alto nível de proteção.

3.9.4.2. A CONTRATADA será responsável por operar, configurar, gerenciar, integrar, atender requisições, mudanças e monitorar as soluções existentes na PRODEB e elencadas neste Termo de Referência;

3.9.4.2.1. Todas as ferramentas, softwares, desenvolvimento de integrações através das APIs disponibilizadas pelos fabricantes e demais soluções necessárias para prestação do serviço de gerenciamento, configuração, integração e monitoramento das soluções de segurança da PRODEB serão de responsabilidade da CONTRATADA e deverão ser disponibilizados sem ônus para a CONTRATANTE;

3.9.4.2.2. Os serviços de operação, configuração e atendinento às mudanças e requisições dizem respeito e não se limitam a: a aplicação de regras, políticas, configurações, exceções, execução de scripts e procedimentos, execução de tefefas estabelecidas no fluxo de mudança, solicitações enviadas pelas equipes e clientes da CONTRATANTE nas soluções e produtos de segurança instalados no Datacenter da CONTRATANTE;

3.9.4.2.3. Os serviços de gerenciamento dizem respeito, e não se limitam a manutenção do pleno funcionamento das soluções e produtos de segurança instalados no Datacenter da Prodeb;

3.9.4.2.4. Os serviços de integração e automatização se referem, e não se limitam a, realizar por meio de configuração, script, API ou sistema gerenciado, a integração entre as soluções e produtos de segurança para aprimoramento e otimização da proteção do ambiente e a automatização das ações de respostas a possíveis incidentes com atuação imediata independente de um operador humano;

3.9.4.3. O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares estritamente necessários à consecução dos serviços aqui elencados é de inteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;

3.9.4.4. Todos os equipamentos e softwares ofertados pela CONTRATADA, quando for o caso, e necessário à consecução das atividades de segurança, devem atender às especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

3.9.4.5. Todos os equipamentos, quando for o caso e necessário à prestação dos serviços, devem ser novos e de primeiro uso. Além disso, os equipamentos e softwares não podem constar, no momento da apresentação da proposta técnica, em listas de end-of-sale, end-of-support, end-of-life ou similares do fabricante, ou seja, não podem ter previsão de descontinuidade de fornecimento, suporte ou vida;

3.9.4.6. Os softwares ofertados pela CONTRATADA devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante;

3.9.4.7. O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade;

3.9.4.8. Para que seja possível o acompanhamento, auditoria e direcionamento de ações no ambiente deverá ser fornecido, ao CONTRATANTE, acesso a console dos produtos e ferramentas que irão compor o serviço de gerenciamento, configuração, operação, atendimento de requisições, integração e monitoramento. para que seja possível o acompanhamento, auditoria e direcionamento de ações no ambiente;

3.9.4.9. Todos os hardware/software a serem utilizados para atendimento às exigências de serviços deste Termo de Referência deverão ser apresentados de forma clara na proposta comercial e deverão estar acompanhados de comprovação técnica através de documentação oficial e pública emitida pelo fabricante das soluções;

3.9.4.10. A CONTRATADA deverá disponibilizar à CONTRATANTE, Painel Central de Informações e Gerência das Soluções, permitindo monitorar em conjunto com o Centro de Operação de Segurança da Informação da CONTRATANTE que devem ocorrer 24x7 em regime remoto. É de responsabilidade da CONTRATADA manter as informações do Painel Central sempre atualizadas e em operação.

3.9.4.11. A CONTRATADA terá um prazo de até 60 (sessenta) dias para implementar o Centro de Operações após a emissão de Órdem de Serviço.

3.9.4.12. Este serviço deverá monitorar e gerenciar e integrar as soluções de segurança da informação elencadas neste Termo de Referência, bem como as suas atualizações durante o período de vigência de contrato.

3.9.4.13. A CONTRATADA deverá avaliar situações em que o ambiente esteja sob ataque ou risco iminente de ataque, provendo o conhecimento e experiência necessários para recomendar possíveis medidas de preparação, mitigação, contenção, defesa e resposta.

3.9.4.14. Os serviços comportarão monitoramento, operação, atendimento de requisições, administração e suporte de todos as soluções elencadas neste Termo de Referência.

3.9.4.15. A CONTRATADA será responsável por apoiar o processo de Resposta a Incidentes de Segurança.

3.9.4.16. A CONTRATADA deverá produzir relatórios de Incidentes de Segurança.

3.9.4.17. Deverá realizar apresentação de relatório mensal com análise dos indicadores de comprometimento e anomalias detectadas e recomendações para melhoria dos modelos de correlação aplicados para detecção de ameaças.

3.9.4.18. Deverá realizar apresentação de relatório mensal com análise de tendências de incidentes de segurança da informação.

3.9.4.19. O acesso ao centro de operações e às soluções da CONTRATADA e da CONTRATANTE devem ser restrito apenas a funcionários autorizados.

3.9.4.20. A CONTRATADA deverá manter atualizados os softwares destinados à execução dos serviços, implementando as últimas versões estáveis, atualizações e correções recomendadas pelo fabricante, de modo a assegurar a plena integridade, segurança e o desempenho do ambiente em produção.

3.9.4.21. Deverão ser realizadas reuniões trimestrais gerenciais para avaliação e acompanhamento dos serviços contratados.

3.9.4.22. A CONTRATADA e a CONTRATANTE deverão, em conjunto, criar e revisar periodicamente os processos, procedimentos operacionais e instruções de trabalho de segurança, realizando as adaptações e evoluções necessárias.

3.9.4.23. A CONTRATADA deverá disponibilizar à CONTRATANTE serviço para abertura e acompanhamento de requisições, mudanças e incidentes que deverá estar acessível durante 24 horas

por dia, 7 dias por semana, 365 dias por ano, sem ônus adicional para a CONTRATANTE, constituído de no mínimo:

3.9.4.23.1. Serviço de atendimento com discagem gratuita (0800) e ou de custo local para telefone fixo (DDD 71).

3.9.4.23.2. E-mail.

3.9.4.23.3. Abertura de ticket através solução de gestão de incidentes da CONTRATADA.

3.9.4.24. Não haverá limitação no número de chamados que poderão ser abertos.

3.9.4.25. A CONTRATADA manterá registro de todas as ordens de serviço abertas, disponibilizando, para cada uma, no mínimo as seguintes informações:

3.9.4.25.1. Número sequencial da ordem.

3.9.4.25.2. Data e hora de abertura.

3.9.4.25.3. Severidade.

3.9.4.25.4. Descrição do problema.

3.9.4.25.5. Item de configuração associado

3.9.4.25.6. Responsável pela abertura do chamado

3.9.4.25.7. Responsável pelo atendimento do chamado

3.9.4.25.8. Tipo do chamado (requisição, incidente ou requisição de mudança)

3.9.4.25.9. Data e hora do início do atendimento.

3.9.4.25.10. Data e hora de término do atendimento (solução)

3.9.4.25.11. Auditoria de todo o fluxo e atendimentos feitos;

3.9.4.26. O monitoramento de disponibilidade dos ativos do ambiente da CONTRATANTE, elencados neste Termo de Referência, deverá ser realizado através de ferramenta (hardware e/ou software) que coletará as informações necessárias para garantir que as soluções estejam sempre ativas e operantes.

3.9.4.27. Deve ser elaborado e enviado mensalmente um relatório executivo com o resumo das principais ocorrências e as providências executadas pela CONTRATADA, além de gráficos e estatísticas relativos à conformidade operacional do ambiente. A formatação deste relatório deve estar em comum acordo com a CONTRATANTE.

3.9.4.28. A manutenção visa manter em perfeito estado de operação os serviços fornecidos em atendimento ao objeto, deste modo a CONTRATADA deve cumprir os seguintes procedimentos:

3.9.4.28.1. Desinstalação, reconfiguração ou reinstalação decorrentes de falhas de software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados.

3.9.4.28.2. Quanto às atualizações pertinentes aos softwares, entende-se como "atualização" a aplicação de toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas releases, versions, builds, upgrades, englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia das soluções elencadas neste TR.

3.9.4.28.3. Para servidores, a CONTRATADA deverá manter índice de atualização do conteúdo de segurança (ex: assinaturas) e engines/motores de detecção de EPP e EDR acima de 100%, desde que suportadas pelo sistema operacional do endpoint e que o acesso às máquinas seja facultado à CONTRATADA pela CONTRATANTE. Este indicador deve ser extraído da própria console de gerenciamento da solução.

3.9.4.28.4. Manutenção da conformidade, de forma automatizada, de estações de trabalho, servidores e dispositivos de rede (switches e firewalls), conforme as especificações de conformidade da CONTRATANTE. As eventuais alterações de configuração e/ou instalação de software de forma automatizada deverão ser previamente autorizadas pela CONTRATANTE.

3.9.4.28.5. Implementação de políticas de controle de acesso à rede conforme definições da CONTRATANTE.

3.9.4.28.6. A operação e administração (gerenciamento total) das soluções será realizada pela CONTRATADA conforme as orientações e solicitações de configurações e políticas realizadas pela Equipe de Segurança da CONTRATANTE.

3.9.4.29. As solicitações de alteração de configurações deverão ser realizadas conforme o ANS definido na Seção – Acordo de Nível de Serviço – ANS.

3.9.4.30. No caso de necessidade de ações preventivas ou corretivas a CONTRATADA agendará com antecedência junto a CONTRATANTE as implementações das correções, fora do horário comercial, preferencialmente em feriados e finais de semana. Nenhuma ação poderá ser executada no ambiente sem a ciência e anuência do CONTRATANTE.

3.9.4.31. A CONTRATADA deverá seguir o processo de mudança estabelecido pelo CONTRATANTE. Sempre que solicitado, a CONTRATADA deverá estar disponível para participar das reuniões com o Comitê de Mudanças, para prestar informações sobre os ambientes e serviços por elas executados.

3.9.4.32. Mudanças que impliquem em um conjunto de procedimentos complexos, que envolvam várias equipes ou empresas contratadas e que implicarem em riscos de paralisação de quaisquer serviços considerados prioritários, deverão ser tratadas como um Projeto.

3.9.4.33. A CONTRATADA deverá apresentar a CONTRATANTE a proposta de todas as mudanças no ambiente, conforme níveis de controle estabelecidos. Para todas as mudanças apresentadas, será necessário acompanhar, dentre outras informações, as análises de risco relativas às mudanças, descrevendo o impacto da sua realização.

3.9.4.34. As manutenções programadas, que impliquem em extensiva parada do ambiente, serão realizadas durante um final de semana. Tais atividades realizadas fora do horário regular não ensejarão qualquer pagamento adicional em relação ao estabelecido no contrato, portanto a CONTRATADA deverá prever esta situação em sua composição de custos.

3.9.4.35. A CONTRATADA será responsável pela aplicação de controles de segurança adequados (criptografia) para garantir a confidencialidade de qualquer dado ou informação do CONTRATANTE que receber em seu ambiente ou em terceiro contratado.

3.9.4.36. A CONTRATADA deverá comunicar formalmente o CONTRATANTE sempre que identificar algum serviço com falhas de implementação e que tornem o ambiente vulnerável a indisponibilidade.

3.9.4.37. A CONTRATADA deverá prestar suporte a todos os componentes de software elencados neste TR para a implementação e utilização da solução.

3.9.4.38. Os serviços de monitoramento, suporte técnico, manutenção e resposta a incidentes deverá ser prestado por profissional devidamente certificado nas soluções tecnológicas elencadas neste Termo de Referência.

3.9.4.39. A CONTRATADA deverá contar com funcionários capacitados para a realização das atividades de monitoramento de redes e análise e resposta a incidentes de segurança, conforme quadro mínimo de pessoal e certificações exigidas neste TR.

3.9.4.40. Caso a Equipe de Atendimento Técnico da CONTRATADA sofra alguma alteração em sua composição durante a vigência deste contrato, tal fato deve ser imediatamente informado ao gestor do contrato, incluindo as respectivas comprovações acerca dos requisitos de qualificação exigidos para esses profissionais e as informações necessárias para liberação do acesso dos técnicos às soluções e dependências da PRODEB.

3.9.4.41. As informações relacionadas ao ANS estão na Seção – Acordo de Nível de Serviço – ANS.

3.9.4.42. Ao final, ou em qualquer hipótese de encerramento antecipado do contrato, a CONTRATADA deverá repassar à CONTRATANTE todo o conhecimento técnico e de processos utilizados na prestação dos serviços. Além disso deverão ainda ser revogados todos os acessos dos prepostos da CONTRATADA aos equipamentos e serviços da CONTRATANTE, bem como caixas postais e perfis criados no ambiente da CONTRATANTE para a prestação dos serviços.

3.9.5. SERVIÇOS DE GESTÃO DE VULNERABILIDADES

3.9.5.1. Serviço de gestão de vulnerabilidades tem por objetivo Serviço de gestão de vulnerabilidades, que tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação no ambiente a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas;

3.9.5.2. No início da atuação da CONTRATADA, em até 30 dias após a emissão da Ordem de Serviço, deverá realizar um diagnóstico inicial das vulnerabilidades existentes, utilizando as soluções disponibilizadas pela CONTRATANTE, e encaminhá-lo à Equipe Técnica da CONTRATANTE, sob forma de relatório detalhado, incluindo a construção da Matriz de Responsabilidades e as recomendações e procedimentos de correção/mitigação.

3.9.5.3. Este serviço tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações da PRODEB, a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas.

3.9.5.4. A CONTRATADA deverá realizar checagens (scans) e varreduras nos ativos, aplicações, servidores e recursos da CONTRATANTE. A CONTRATANTE será responsável pelo tratamento contínuo das vulnerabilidades encontradas na infraestrutura e aplicações da PRODEB, com o apoio das informações para correção geradas pela CONTRATADA.

3.9.5.5. Após o término das rotinas de checagens (scans) e varreduras no ambiente, deverá a CONTRATADA realizar uma análise de falso positivo das vulnerabilidades descobertas, isso quer dizer, que devem ser informadas à CONTRATANTE apenas vulnerabilidades que existam de fato em seu ambiente.

3.9.5.6. Após análise de falso positivo, a CONTRATADA deverá informar à CONTRATANTE as vulnerabilidades encontradas e os meios de mitigação destas vulnerabilidades, inclusive soluções de contorno quando não houver soluções conhecidas.

3.9.5.6.1. Medidas de contorno podem ser, por exemplo, criação de regras de isolamento dos ativos vulneráveis em firewall, WAF, IPS, XDR, EDR ou outros controles disponibilizados pela CONTRATANTE.

3.9.5.7. Para vulnerabilidades encontradas no ambiente que já sejam conhecidas e catalogadas (CVE, CVSS e outras bases de vulnerabilidades conhecidas), a CONTRATADA deverá apresentar relatório especificando a vulnerabilidade e propondo a solução, como por exemplo, a aplicação de patch do fabricante ou aplicação de blindagem por meio de patch virtual.

3.9.5.8. Como último passo, a CONTRATADA deverá atualizar todos os controles e indicadores, conforme descritos abaixo.

Denominação	Forma de Cálculo	Filtro	Agrupador	Descrição
Quantitativo de vulnerabilidades	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	Número total de vulnerabilidades
Quantitativo de vulnerabilidades críticas por área responsável	Soma de vulnerabilidades críticas por área responsável	Vulnerabilidades críticas	Vulnerabilidades	Número total de vulnerabilidades críticas por área responsável
Quantitativo de vulnerabilidades corrigidas	Soma de vulnerabilidades corrigidas	Vulnerabilidades corrigidas	Vulnerabilidades	Número total de vulnerabilidades corrigidas
Quantitativo de vulnerabilidades em Aplicações WEB	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB
Quantitativo de vulnerabilidades corrigidas em aplicações WEB	Soma de vulnerabilidades corrigidas em aplicações WEB	Vulnerabilidades corrigidas em aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades corrigidas em Aplicações WEB
Quantitativo de vulnerabilidades em ativos	Soma de vulnerabilidades em ativos	Vulnerabilidades em ativos	Vulnerabilidades	Número total de vulnerabilidades em ativos
Quantitativo de vulnerabilidades corrigidas em ativos	Soma de vulnerabilidades corrigidas em ativos	Vulnerabilidades corrigidas em ativos	Vulnerabilidades	Número total de vulnerabilidades corrigidas em ativos
Quantidade de vulnerabilidades em códigos de aplicações	Soma de vulnerabilidades em códigos de aplicações	Vulnerabilidades em códigos de aplicações	Vulnerabilidades	Número total de vulnerabilidades em códigos de aplicações
Quantitativo de certificados digitais expirados	Soma de certificados digitais expirados	Certificados digitais expirados	Certificados digitais	Número total de certificados digitais expirados
Quantitativo de certificados digitais a expirar em 3 meses	Soma de certificados digitais a expirar em 3 meses	Certificados digitais a expirar em 3 meses	Certificados digitais	Número total de certificados digitais a expirar em 3 meses

Denominação	Forma de Cálculo	Filtro	Agrupador	Descrição
TOP 10 – Ativos mais vulneráveis	Soma de vulnerabilidades por ativo	Vulnerabilidades por ativo	Vulnerabilidades	TOP 10 do número de vulnerabilidades por ativo
TOP 10 – Aplicações WEB mais vulneráveis	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB
TOP 10 – Aplicações WEB mais vulneráveis em comparação com OWASP	Soma de vulnerabilidades em Aplicações WEB em comparação com OWASP	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB em comparação com OWASP

3.9.5.9. O processo descrito é o mínimo esperado a ser seguido e executado pela CONTRATADA todavia como o objeto do presente Termo de Referência se trata de um serviço continuado, logo se espera da CONTRATADA a apresentação da melhoria contínua deste, a qual pode ser alterado desde que aprovado pela CONTRATANTE.

3.9.5.10. O ciclo de vida do processo de gestão de vulnerabilidade deve ser executado de forma recorrente. O início do processo não se limita apenas em rotinas de tempo definidas, mas poderá a CONTRATANTE também solicitar análises sob demanda durante a vigência contratual.

3.9.6. SERVIÇOS DE MONITORAMENTO DE SEGURANÇA, GESTÃO DE INCIDENTES DE SEGURANÇA E RESPOSTA A ATAQUES CIBERNÉTICOS

3.9.6.1. Este serviço tem o objetivo de monitorar de forma contínua e ininterrupta todas as soluções de segurança instaladas no ambiente da CONTRATANTE para identificação de ataques cibernéticos direcionados à PRODEB;

3.9.6.2. Deve trabalhar conjuntamente com a equipe de Segurança da CONTRATANTE a fim de otimizar o processo de resposta ao incidente, minizando os impactos para o negócio;

3.9.6.3. Este serviço deve analisar, documentar e indicar como conter e como remediar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado obedecendo aos frameworks NIST e SANS de resposta a incidente de segurança da informação e boas práticas de mercado.

3.9.6.4. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade, Disponibilidade e Privacidade.

3.9.6.5. O serviço de resposta a incidentes será responsável por monitorar equipamentos e softwares componentes das soluções de segurança da CONTRATANTE, envolvendo identificação, classificação e análise de eventos que possam comprometer a disponibilidade, integridade, confidencialidade dos serviços e requerimentos legais de privacidade dos serviços.

3.9.6.6. A CONTRATADA deverá prover serviços de resposta aos incidentes de segurança da informação diante os eventos registrados no monitoramento.

3.9.6.7. Os serviços de monitoramento e resposta a incidentes de segurança poderão ser prestados REMOTAMENTE por meio de Centro de Operações de Segurança da Informação, sem prejuízo aos níveis de serviços solicitados nesse documento.

3.9.6.8. O regime de execução deste serviço deverá ser 24x7 (vinte e quatro horas por dia, sete dias por semana.

3.9.6.9. O monitoramento de segurança deverá ser autônomo (automatizado) e realizado através de ferramentas próprias da CONTRATANTE integradas via API com as consoles/servidores de

gerenciamento para automação de coleta de alertas críticos nas soluções elencadas neste Termo de Referência e com acionamento imediato da equipe da CONTRATADA.

3.9.6.10. A ocorrência de alertas de alta criticidade devem acionar diretamente, de forma automática, através de alarme sonoro em aplicativo de celular, os técnicos de plantão da CONTRATADA para início imediato do tratamento da ocorrência, dentro dos prazos definidos no ANS, sendo reportados imediatamente ao preposto da CONTRATANTE para ciência do fato, além de abrir imediatamente um ticket na solução de gestão de incidentes da CONTRATADA.

3.9.6.11. Todos os alertas gerados pelo monitoramento autônomo deverão ser enriquecidos de informações para detalhamento da ocorrência e orientações de como mitigar e tratar o alerta através de Inteligência Artificial Generativa, com desempenho igual ou superior ao ChatGPT 4 (ex: Google Bard ou Claude 2).

3.9.6.12. A ocorrência de um alerta detectado pelo monitoramento autônomo deverá resultar na abertura imediata de um ticket para tratamento do incidente, notificação por e-mail e alarme em celular às equipes envolvidas no processo e abertura de processo de gestão de incidentes em plataforma de BPMn para acompanhamento preciso dos Níveis de Serviço.

3.9.6.13. O ticket aberto para tratamento do incidente bem como os e-mails de notificação deverá conter todas as informações produzidas pela Inteligência Artificial Generativa para auxiliar a equipe de resposta a incidentes na rápida mitigação da ocorrência.

3.9.6.14. A PRODEB deverá ter acesso a todos os tickets, bem como o detalhamento das ações realizadas para o seu tratamento, diretamente na solução de gerenciamento de incidentes da CONTRATADA.

3.9.6.15. A CONTRATADA deverá informar mensalmente a escala de técnicos de sobreaviso que atenderão os alertas de alta criticidade durante o período do plantão 24x7.

3.9.6.16. À opção da CONTRATANTE, esta poderá indicar os profissionais para receberem os alarmes em tempo real, de forma simultânea, no aplicativo de celular a ser fornecido pela CONTRATADA sem custos adicionais.

3.9.6.17. O tratamento das ocorrências críticas geradas pelo sistema de monitoramento automático deve ser acompanhado através de plataforma de gestão automatizada de processos (BPMn), que indique claramente e controle os prazos para execução de cada etapa do processo de resposta aos incidentes detectados.

3.9.6.18. O processo de tratamento dos incidentes deve poder ser customizado na plataforma de BPMn da CONTRATADA para melhor atender às necessidades específicas da CONTRATANTE,

3.9.6.19. Os dados de SLA do tratamento de incidentes, incluindo o SLA de cada uma de suas etapas, deve ser disponibilizado em tempo real para a contratada através de dashboards gráficos.

3.9.6.19.1. O processo de tratamento de incidentes deve conter pelo menos as seguintes características:

3.9.6.19.2. Notificação automática e imediata da CONTRATADA sobre a ocorrência detectada.

3.9.6.19.3. Abertura

3.9.6.19.4. Investigação da ocorrência através dos recursos fornecidos pela solução.

3.9.6.19.5. Determinação da real criticidade do incidente.

3.9.6.19.6. Execução de ações de contenção previamente acordadas com o cliente.

3.9.6.20. O processo automatizado deve ser capaz de tratar de forma diferenciada pelo menos 4 níveis de criticidade de alertas.

3.9.6.21. O processo automatizado deve ser capaz de enviar e-mail e alertas em aplicativo de celular de forma automática para a CONTRATADA e para a CONTRATANTE.

3.9.6.22. O processo automatizado deve ser capaz de emitir avisos sonoros através de aplicativo de celular para os técnicos da CONTRATADA e da CONTRATANTE, com diferentes graus de intensidade a depender do nível de criticidade da situação detectada.

3.9.6.23. Deve permitir a customização, para cada solução da CONTRATANTE, de quais tipos de alertas se enquadram em cada um dos níveis de criticidade.

3.9.6.24. Deve ser disponibilizado para a CONTRATANTE um dashboard de acompanhamento em tempo real dos processos de tratamento dos incidentes que apresente, no mínimo:

3.9.6.24.1. Tarefas em aberto com indicação do responsável pela sua execução e tempo restante para sua finalização de acordo com o ANS contratado.

3.9.6.24.2. Tarefas em atraso com indicação do responsável pela sua execução e tempo de atraso em relação ao ANS contratado.

3.9.6.24.3. Tabela de atraso médio de tarefas já encerradas.

3.9.6.24.4. Tabela de tempo médio de execução de tarefas já encerradas.

3.9.6.25. O monitoramento de segurança deverá contemplar o correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, conforme definido em processo de gestão de incidentes.

3.9.6.26. Além do monitoramento da ferramenta de análise avançada de logs e pacotes de rede, a CONTRATADA deverá realizar o monitoramento de log e eventos de segurança das soluções de XDR, NGFW, WAF (Web Application Firewall), endpoint EDR e emulação e identificação de malware (sandbox) elencadas neste TR e outras soluções que vierem a integrar o ambiente de segurança da CONTRATANTE.

3.9.6.27. Para execução do serviço, a CONTRATADA será responsável pela integração, por meio da coleta de logs/eventos, da solução de análise avançada de logs e pacotes de rede com as demais soluções de segurança instaladas no ambiente da CONTRATANTE

3.9.6.28. Após o incidente de segurança aberto, será de responsabilidade do grupo de resposta a incidente de segurança da CONTRATADA, analisar os logs e artefatos enviados, a fim de no primeiro instante identificar as fontes geradoras de tais logs.

3.9.6.29. Uma vez realizada as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança da CONTRATADA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.

3.9.6.30. Como próximo passo o grupo de resposta a incidente de segurança da CONTRATADA, deverá comunicar ao time de segurança da informação do CONTRATANTE, de acordo com os SLAs informados nesse documento, as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente. Dados e Informações iniciais esperados da CONTRATADA:

3.9.6.30.1. Prioridade: Representação/número de prioridade ou severidade do incidente, em uma escala de 1 a 4 sendo 1 a maior prioridade.

3.9.6.30.2. Categoria/Classificação: Palavra única que classifica o tipo do incidente, como malware, phishing, misconfiguration entre outros.

3.9.6.30.3. Entidades fontes: Se aplicável, os detalhes dos nomes dos dispositivos, endereço de e-mails, endereços IPs, detalhes da vulnerabilidade ou outros fatores de identificação que apontam para a fonte do incidente.

3.9.6.30.4. Entidades de destino: Os detalhes de nomes dos dispositivos, endereços de e-mail, endereços IPs ou outros fatores de identificação que apontam para os ativos afetados.

3.9.6.30.5. Ações recomendadas: Instruções inteligentes e simples a serem seguidas que detalhem as ações de remediação já tomadas pela CONTRATADA e ações que a CONTRATANTE precisa tomar. O nível de autonomia para execução de ações no ambiente da CONTRATANTE deverá ser objeto de política específica a ser definida no início da execução do contrato.

3.9.6.30.6. Fontes da Detecção: Detalhes das fontes dos logs ou os dispositivos de segurança que identificaram (ou colaboraram) na descoberta do incidente. Essa informação será útil para análise de causa raiz ou remediação direcionada.

3.9.6.31. Juntamente com o CONTRATANTE o grupo de resposta a incidente de segurança da CONTRATADA, deverá definir a severidade do incidente de segurança. A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente.

3.9.6.32. Após análises iniciais do incidente, caberá ao grupo de resposta a incidente de segurança, realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

3.9.6.33. Todo o processo de análise e os resultados obtidos devem ser documentados a todo tempo na ferramenta de gestão de incidente da segurança da informação da CONTRATANTE, para que o CONTRATANTE acompanhe todos os passos para a solução do incidente.

3.9.6.34. Uma vez identificado o comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança da CONTRATADA, deverá definir uma estratégia para a mitigação e contenção do ataque em questão. Caso seja necessário qualquer tipo de alteração no parque computacional do CONTRATANTE, para contenção e mitigação do incidente, deverá obedecer aos níveis de autonomia da CONTRATADA definidos no início do contrato.

3.9.6.35. Mitigado o incidente de segurança, o próximo passo exigido é que a CONTRATADA, através do grupo de resposta a incidente de segurança, inicie o processo de recolhimento de toda e quaisquer

evidências, e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

3.9.6.36. Inicia-se então o processo de restauração dos serviços e soluções afetadas. Este processo será realizado pela CONTRATANTE, com o apoio da CONTRATADA.

3.9.6.37. Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense. Tal análise deve ser realizada com o objetivo de identificar (pessoas, locais e/ou eventos), correlacionando todas as informações reunidas, e gerando como produto final um laudo sobre o incidente de segurança em questão.

3.9.6.38. O laudo deverá conter, além das informações técnicas do incidente, a sua classificação conforme a tabela a seguir:

PERSPECTIVA	CLASSE	DESCRIÇÃO
Quanto a Natureza	Evento	Algo que ocorreu nos Sistemas de Informações, Infraestrutura ou Dados, mas não é necessariamente malicioso ou que requer uma ação.
	Alerta	Algo potencialmente acionável. Uma indicação de um evento acionável.
	Incidente	Qualquer evento com a violação da confidencialidade, integridade, disponibilidade e privacidade, mas **sem impacto à missão ou ao negócio da organização.**
	Incidente Grave	Qualquer evento com violação da confidencialidade, integridade, disponibilidade e privacidade, **com impacto à missão ou ao negócio.**
	Invasão e/ou Vazamento	Perda ou comprometimento de sistemas, dados regulados, ou de propriedade empresarial que dispara uma ação ou resposta legal que vá além dos serviços de monitoramento e resposta a incidentes.
Quanto ao Impacto de Negócio	Nenhum	Nenhum efeito na capacidade da organização de oferecer todos os serviços a todos os usuários.
	Baixo	Efeito mínimo; a organização ainda pode fornecer todos os serviços críticos a todos os usuários, mas perdeu eficiência.
	Médio	A organização perdeu a capacidade de fornecer um serviço essencial e crítico para um subconjunto de usuários do sistema.
	Alto	A organização não é mais capaz de fornecer alguns serviços essenciais e críticos a nenhum usuário e/ou houve comprometimento de dados institucionais e/ou pessoais.

	Crítico	A organização não é mais capaz de fornecer alguns serviços essenciais e críticos a nenhum usuário e/ou houve comprometimento de dados institucionais e/ou pessoais.
Quanto ao Impacto de Informações	Nenhum	Nenhuma informação foi exfiltrada, alterada, apagada ou, de qualquer outra forma, comprometida
	Quebra de Privacidade	Informações sensíveis pessoalmente identificáveis (PII), foram acessadas ou exfiltradas.
	Quebra de Propriedade	Informações proprietárias não classificadas, tais como informações de infraestrutura crítica protegida (PCII), foram acessadas ou exfiltradas
	Perda de Integridade	Informações sensíveis ou proprietárias foram alteradas ou excluídas
	Quebra de Privacidade	Informações sensíveis pessoalmente identificáveis (PII), foram acessadas ou exfiltradas.
	Quebra de Propriedade	Informações proprietárias não classificadas, tais como informações de infraestrutura crítica protegida (PCII), foram acessadas ou exfiltradas
	Perda de Integridade	Informações sensíveis ou proprietárias foram alteradas ou excluídas.
	Quebra de Privacidade	Informações sensíveis pessoalmente identificáveis (PII), foram acessadas ou exfiltradas.
Quanto ao Impacto de Recuperação	N/A	Não se aplica
	Regular	O tempo para recuperação é previsível com os recursos existentes.
	Complementado	O tempo para recuperação é previsível com recursos adicionais.
	Estendido	O tempo para recuperação é imprevisível; são necessários recursos adicionais e ajuda externa.
	Não Recuperável	A recuperação do incidente não é possível (por exemplo, os dados sensíveis exfiltrados são publicados; lançar investigação para apuração crimina

3.9.6.39. O grupo de resposta a incidente de segurança da CONTRATADA, deve documentar na ferramenta de incidente de segurança, as lições aprendidas do incidente de segurança em questão, formando

durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos.

3.9.6.40. O processo descrito é o mínimo esperado a ser seguido e executado pela CONTRATADA, todavia como o objeto deste Termo de Referência se trata de um serviço continuado, logo se espera da CONTRATADA a apresentação da melhoria contínua deste, a qual pode ser alterado desde que aprovado pela CONTRATANTE.

3.9.7. SERVIÇOS DE INTEGRAÇÃO DE INFORMAÇÕES DE INTELIGÊNCIA SOBRE AMEAÇAS (THREAT INTELLIGENCE):

3.9.7.1. Coletar diariamente informações de pelo menos 20 fontes relevantes de inteligência sobre ameaças (cyber threat intelligence feeds) disponíveis pelo mundo, de categorias como phishing, códigos maliciosos, botnets, internet profunda (deep web), spam, ataques APT (advanced persistent threats), ransomware etc.;

3.9.7.2. Correlacionar as informações coletadas, utilizando plataforma de big data para processamento visando normalizar e desduplicar informações, gerando listas acionáveis de inteligência contra am eaças;

3.9.7.3. Integrar as listas no serviço de Monitoramento e Resposta a Incidentes, no intuito de aprimorar a capacidade da detecção de incidentes e diminuir falso-positivos;

3.9.7.4. Monitorar ameaças emergentes e avaliar a aplicabilidade especificamente no ambiente do CONTRATANTE, propondo proativamente a realização de contramedidas com o objetivo de prevenir a exploração de alguma brecha de segurança;

3.9.7.5. A solução deve ser capaz de detectar em tempo real, ameaças alimentadas pelas seguintes bases de inteligência:

3.9.7.5.1. relatórios de ameaças e segurança;

3.9.7.5.2. relatórios de botnets e centros de Comando e Controle;

3.9.7.5.3. identificação de exploit kits;

3.9.7.5.4. indicadores de ataques "zeroday";

3.9.7.5.5. indicadores de comprometimento, suspeitas e avisos Informativos;

3.9.7.5.6. inteligência de tendências;

3.9.7.5.7. proxies anônimos;

3.9.7.5.8. classificação de sites;

3.9.7.5.9. endereços de rede TOR

3.9.8. SERVIÇOS DE VALIDAÇÃO CONTÍNUA DE SEGURANÇA

3.9.8.1. Serviços de simulação de ataques cibernéticos para identificação de gaps de proteção, alerta e bloqueio de forma continuada e geração de recomendações para mitigar os gaps encontrados.

3.9.8.2. A CONTRATADA deverá fornecer um serviço de Validação de Controle de Segurança. Este serviço deve incluir a medição e o fortalecimento da resiliência cibernética, testando automaticamente e continuamente a eficácia das ferramentas de segurança através de uma solução automatizada específica para esta finalidade.

3.9.8.3. A CONTRATADA deverá fornecer um serviço que simula ameaças cibernéticas do mundo real para identificar lacunas de prevenção e detecção. Este serviço deve incluir a obtenção de recomendações de mitigação acionáveis para abordá-las de forma rápida e eficaz.

3.9.8.4. A CONTRATADA deverá fornecer um serviço de realização de simulações de violação e ataque para testar a eficácia das medidas de segurança existentes e identificar áreas de melhoria.

3.9.8.5. A CONTRATADA deverá fornecer um serviço que testa a prontidão de segurança contra mais de 3.800 ameaças, incluindo malware, ransomware e APTs.

3.9.8.6. A CONTRATADA deverá fornecer um serviço que valida a preparação contra as últimas ameaças. Este serviço deve incluir a identificação de fraquezas de prevenção e detecção de ameaças, avaliando a eficácia das ferramentas de segurança por meio de simulações agendadas continuamente.

3.9.8.7. A CONTRATADA deverá fornecer um serviço que mapeia os resultados da avaliação para o Framework MITRE ATT&CK, permitindo a visualização da cobertura de ameaças e a priorização da mitigação de lacunas.

3.9.8.8. A CONTRATADA deverá fornecer um serviço que fornece métricas em tempo real, incluindo uma pontuação de segurança geral para a organização, ajudando a medir o desempenho e provar o valor dos investimentos já realizados em segurança da informação.

3.9.8.9. A CONTRATADA deverá fornecer um serviço que automatiza os processos de avaliação e engenharia manual para reduzir a fadiga e ajudar as equipes de segurança a trabalharem juntas de forma mais colaborativa.

3.9.8.10. A CONTRATADA deverá fornecer um serviço que automatiza a validação de controle de segurança incluindo a simulação de ameaças, a validação de eficácia e a mitigação de lacunas de forma segura, simples e contínua.

3.9.8.11. A CONTRATADA deverá fornecer um serviço de avaliação e relatório automáticos do nível de proteção contra ameaças proporcionado pelos controles de segurança. Este serviço deve incluir a identificação de vulnerabilidades e a avaliação da eficácia dos controles de segurança existentes.

3.9.8.12. A CONTRATADA deverá fornecer um serviço de consultoria para fornecer conselhos de mitigação para brechas de segurança identificadas. Este serviço deve incluir a análise de incidentes de segurança e a recomendação de medidas de mitigação.

3.9.8.13. A CONTRATADA deverá fornecer um serviço de medição eficiente da detecção de incidentes de segurança da informação. Este serviço deve incluir a monitorização contínua do ambiente de datacenter e a geração de relatórios sobre incidentes de segurança.

3.9.8.14. A CONTRATADA deverá fornecer um serviço de consultoria para fornecer conselhos adequados sobre detecção de ameaças para incidentes não detectados. Este serviço deve incluir a análise de ameaças potenciais e a recomendação de medidas de detecção.

3.9.8.15. A CONTRATADA deverá fornecer um serviço de simulação de ataques cibernéticos para avaliar a segurança. Este serviço deve incluir a realização de simulações de violação e ataque para testar a eficácia das medidas de segurança existentes e identificar áreas de melhoria.

3.9.8.16. A CONTRATADA deverá fornecer um serviço de automação e integração entre as diferentes soluções de segurança para otimizar a resposta a incidentes. Este serviço deve incluir a implementação de automação e integração entre as diferentes soluções de segurança para permitir uma resposta mais rápida e eficaz a incidentes de segurança.

3.9.8.17. A CONTRATADA deverá fornecer um serviço que permite a execução de simulações paralelas com múltiplos agentes. Este serviço deve incluir a capacidade de executar várias simulações ao mesmo tempo para testar a eficácia das medidas de segurança em diferentes cenários.

3.9.8.18. A CONTRATADA deverá fornecer um serviço de fornecimento de informações adequadas para cada simulação de ataque. Este serviço deve incluir a geração de relatórios detalhados sobre cada simulação de ataque, incluindo os métodos utilizados, os resultados e as recomendações para melhorias.

3.9.8.19. A CONTRATADA deverá fornecer um serviço que permite mostrar cenários de sucesso/falha no framework MITRE ATT&CK em base tática e técnica na interface web. Este serviço deve incluir a capacidade de visualizar os resultados das simulações de ataque em um formato fácil de entender.

3.9.8.20. A CONTRATADA deverá fornecer um serviço de teste da eficácia de segurança dos sistemas de segurança de cliente, rede, virtualização e nuvem da instituição. Este serviço deve incluir a realização de testes para avaliar a eficácia das medidas de segurança em diferentes sistemas e ambientes.

3.9.8.21. A CONTRATADA deverá fornecer um serviço de avaliação do nível de segurança fornecido por um grupo de endpoints e/ou tecnologias de segurança de rede. Este serviço deve incluir a realização de avaliações para determinar a eficácia das medidas de segurança em proteger os endpoints e a rede.

3.9.8.22. O fornecedor deverá fornecer um serviço de simulação de ataques, relatório de descobertas e proposta de mitigações de forma contínua e quase em tempo real. Este serviço deve incluir a realização de simulações de ataque contínuas para testar a eficácia das medidas de segurança e identificar áreas de melhoria.

3.9.8.23. O fornecedor deverá fornecer um serviço de suporte à integração e comunicação com outras soluções baseadas num acesso "Application Control Interface" (API) ou no protocolo Syslog. Este serviço deve incluir a capacidade de integrar e comunicar com outras soluções de segurança para permitir uma resposta coordenada a incidentes de segurança.

3.9.8.24. O fornecedor deverá fornecer um serviço de análise se as ameaças nos vetores de ataque testados são detectadas e alertadas nas soluções "Security Information and Event Management" (SIEM) e Endpoint Detection and Response (EDR). Este serviço deve incluir a capacidade de analisar a eficácia das soluções SIEM e EDR na detecção e alerta de ameaças.

3.9.8.25. A CONTRATADA deverá fornecer um serviço de geração de relatórios individuais de simulação para prevenção e detecção ou apenas para resultados de prevenção nos formatos CSV e PDF sob demanda. Este serviço deve incluir a capacidade de gerar relatórios detalhados sobre as simulações de ataque e as medidas de prevenção e detecção implementadas.

3.9.8.26. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as seguintes Características Gerais:

3.9.8.26.1. Em seu modo de operação normal (sem falhas ou customizações) a solução deve permitir simulações instantâneas e programadas nas seguintes bases: Uma vez, Diariamente, Semanalmente, Mensalmente

3.9.8.26.2. A solução deve ser capaz de executar simulações paralelas com múltiplos agentes.

3.9.8.26.3. A solução deve ser uma solução somente de software para testar automaticamente a eficácia dos controles de segurança usados pela organização por meio dos termos declarados abaixo.

3.9.8.26.4. A solução deve fornecer informações adequadas para cada simulação de ataque de forma que cada ataque possa ser identificado em qualquer um dos dispositivos de segurança em teste.

3.9.8.26.5. A solução deve fornecer acesso à cobertura do framework MITRE ATT&CK na interface web para cada simulação.

3.9.8.26.6. A solução deve fornecer zero resultados falsos positivos, o que significa que qualquer ataque relatado como não impedido pelos controles de segurança instalados pode ser comprovado como tal. Mediante solicitação, o fornecedor realizará os trabalhos necessários para comprovar a veracidade da situação de ataque não prevenido.

3.9.8.26.7. A solução deve ser capaz de testar a eficácia de segurança dos sistemas de segurança de cliente, rede, virtualização e nuvem da instituição, realizando simulações de ataque entre componentes de software que podem ser instalados em uma estrutura distribuída.

3.9.8.26.8. A solução deve ser capaz de avaliar o nível de segurança fornecido por um grupo de endpoints e/ou tecnologias de segurança de rede que funcionam isoladamente ou estão integradas a outros sistemas de segurança, independentemente do fornecedor e da tecnologia subjacentes.

3.9.8.26.9. A solução deve simular ataques, relatar descobertas e ser capaz de propor mitigações de forma contínua e quase em tempo real para cada cenário de ataque.

3.9.8.26.10. Os componentes da solução devem executar simulações de ataque entre seus componentes e não devem iniciar conexões com nenhuma aplicação de produção e sistema de endpoint para fornecer uma avaliação sem riscos, a menos que configurado para movimento lateral.

3.9.8.26.11. As avaliações de controle de segurança de terminal devem ser restritas ao(s) sistema(s) de computador designado(s) e esse processo de avaliação não deve interagir com outros sistemas, a menos que esteja configurado para movimento lateral.

3.9.8.26.12. A solução deverá suportar a integração e comunicar com outras soluções baseadas num acesso "Application Programming Interface" (API) ou no protocolo Syslog para fins como:Relatórios personalizados, Painéis personalizados e Integração com soluções de terceiros como SOAR, SIEM ou outras plataformas.

3.9.8.27. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as seguintes Biblioteca de Ameaças e Templates de Ameaças:

3.9.8.27.1. A solução deve fornecer templates de ameaças estáticos prontos para uso para ameaças emergentes e sugeridas que o usuário também pode modificar para necessidades personalizadas.

3.9.8.27.2. A solução deve fornecer templates de ameaças dinâmicos prontos para uso para gerenciamento de postura de segurança, como prontidão contra ransomwares, prontidão contra grupos APT e racionalização de controle de segurança, como segurança de rede (teste IPS/IDS e NGFW, teste WAF, teste DLP, segurança da Web Teste de gateway), Teste de segurança de endpoint e Teste de segurança de e-mail.

3.9.8.27.3. A solução deverá fornecer os templates dinâmicos mencionados para serem customizados pelo usuário.

3.9.8.27.4. A solução deverá prever a criação customizada de templates dinâmicos com filtros como. Nome da ameaça, tags, categoria de ataque, atores da ameaça, Killchain unificado, táticas MITRE ATT&CK, sistema operacional afetado, gravidade e data de lançamento.

3.9.8.27.5. A solução deve ser capaz de adicionar automaticamente ataques recém-adicionados aos templates dinâmicos sem intervenção do usuário.

3.9.8.27.6. A solução deve usar payloads de ataques maliciosos do mundo real para download de arquivos, e-mail e ataques de aplicações web enquanto testa os controles de segurança da rede.

3.9.8.27.7. As ameaças contidas no banco de dados de tratamento devem ser referenciadas de acordo com o seguinte conjunto de informações, incluindo, mas não se limitando a:

- Número de identificação exclusivo da ameaça (uniqueID)

- Data de lançamento da ameaça
- Uma descrição baseada em texto da ameaça
- A gravidade da ameaça está de acordo com a seguinte escala: Baixa,Médio, Alto.
- Plataformas Afetadas,
- Setor alvo,
- Região segmentada
- Objetivos do atacante,
- Ações,
- Cargas úteis, linhas de comando de processo executadas ou valores de hash com base em tipo de ataque,
- Referências em bancos de dados conhecidos publicamente:virustotal
- Referências nas seguintes classificações de ameaças reconhecidas pelo setor e
- sistemas de enumeração: CVE, CWE, CVSS, OWASP.
- Sistemas operacionais afetados pela ameaça

3.9.8.27.8. A solução permitirá que os resultados da avaliação de ameaças "bloqueadas" e "não bloqueadas" sejam exportados em formato CSV.

3.9.8.28. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as seguintes funcionalidades de Infiltração de rede (FileDownload):

3.9.8.28.1. A solução deve suportar os protocolos HTTP e HTTPS para testar os controles de segurança da rede. Todos os ataques de infiltração de rede aplicáveis (download de arquivo) devem ser executados sobre esses protocolos.

3.9.8.28.2. A solução deve ser capaz de suportar agentes de navegador para testes rápidos de IPS/IDS/Web Gateway sobre HTTPS.

3.9.8.29. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as seguintes funcionalidades de Infiltração de E-mail:

3.9.8.29.1. A solução deve realizar testes SMTP da internet para o domínio corporativo.

3.9.8.29.2. A solução deve realizar ataques de URL usando o protocolo SMTP da internet para o domínio corporativo (e-mail).

3.9.8.29.3. A solução deve suportar um simulador de e-mail sem agente para testes de ataque por e-mail.

3.9.8.30. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as seguintes funcionalidades de Ataque de aplicação web:

3.9.8.30.1. A solução deve executar ataques de aplicações Web em HTTP e HTTPS.

3.9.8.30.2. O banco de dados de ataques da solução deve incluir pelo menos 169 (cento e sessenta e nove) assinaturas exclusivas de ataques de aplicações web na biblioteca de ameaças.

3.9.8.30.3. A solução deve usar o payload real da ameaça para avaliação do controle de segurança, em vez de usar a "reprodução de PCAP" para ataques a aplicações web.

3.9.8.31. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as seguintes funcionalidades de Ataque de Endpoint:

3.9.8.31.1. A solução deve imitar métodos maliciosos usados por APT's (Advanced Persistent Threats) enquanto testa os controles de segurança do endpoint, sem infectar o sistema operacional subjacente.

3.9.8.31.2. A solução deve abranger pelo menos 120 técnicas de framework MITRE ATT&CK Enterprise para sistemas operacionais Windows.

3.9.8.32. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as seguintes funcionalidades de Exfiltração de Dados:

3.9.8.32.1. A solução deve ser capaz de validar soluções DLP de endpoint, email e rede.

3.9.8.32.2. O banco de dados de ataque da solução deve incluir pelo menos 15 (quinze) amostras exclusivas de exfiltração de dados na biblioteca de ameaças.

3.9.8.32.3. A solução deve abranger técnicas de exfiltração pelo menos nos protocolos HTTP, HTTPS e TCP.

3.9.8.32.4. A solução deve abranger pelo menos métodos de ofuscação de criptografia XOR e codificação Base64.

3.9.8.33. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as seguintes funcionalidades de Ataque personalizado:

3.9.8.33.1. A solução deve permitir que os usuários criem ataques de cenário de endpoint do Windows personalizados usando a biblioteca de ação da estrutura MITRE ATT&CK com pelo menos 1000 (mil) ações de cenário de endpoint disponíveis.

3.9.8.33.2. A solução deve permitir que os usuários criem ataques personalizados de infiltração de rede (download de arquivo) usando uma biblioteca de ameaças existente com pelo menos 8.000 (oito mil) arquivos maliciosos disponíveis.

3.9.8.33.3. A solução deve permitir que os usuários criem ataques de aplicações web personalizados usando a biblioteca de ameaças existente com pelo menos 2.000 (dois mil) payloads maliciosos disponíveis.

3.9.8.33.4. A solução deve permitir que os usuários criem ataques de e-mail personalizados usando a biblioteca de ameaças existente com pelo menos 7400 (sete mil e quatrocentos) arquivos maliciosos disponíveis.

3.9.8.33.5. A solução deve permitir que os usuários criem amostras personalizadas de exfiltração de dados usando a biblioteca de ameaças existente com pelo menos 200 (duzentos) arquivos de amostra disponíveis.

3.9.8.33.6. A solução deve permitir que os usuários carreguem seus ataques personalizados para ataques a aplicações web, ataques por e-mail, ataques de infiltração de rede e módulos de ataque de exfiltração de dados.

3.9.8.34. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as seguintes funcionalidades de Mitigação:

3.9.8.34.1. A solução deve exibir o nível de utilização e eficácia da tecnologia de um fornecedor, expresso em porcentagem, número de ameaças bloqueadas e não bloqueadas por simulação.

3.9.8.34.2. A solução deve identificar e associar exclusivamente as assinaturas de mitigação ao conteúdo da biblioteca de ameaças, apresentando um ID de assinatura associado a cada ameaça na biblioteca de ameaças.

3.9.8.34.3. A solução deve apresentar e classificar assinaturas e mitigações por gravidade e categoria (ataques de aplicações web, exploração de vulnerabilidades, códigos maliciosos) das ameaças relacionadas.

3.9.8.34.4. A solução deve permitir a exportação do status de ameaças e assinaturas "não bloqueadas" via formato CSV.

3.9.8.34.5. A solução deve permitir que assinaturas ou ameaças sejam pesquisadas e filtradas usando nomes de ameaças, ações ou assinaturas.

3.9.8.34.6. A solução deve permitir que os usuários filtrem sugestões de mitigação com base em simulações.

3.9.8.34.7. A solução deve permitir que os usuários filtrem as assinaturas do Malware Engine sem moderação para serem exibidas ou ocultadas sob demanda.

3.9.8.34.8. Para brechas de segurança reveladas durante as avaliações de aplicações web e infiltração de rede, a solução deve fornecer sugestões de mitigação específicas do fornecedor em um painel dedicado na interface.

3.9.8.34.9. Para lacunas de segurança reveladas durante as avaliações do cenário de endpoint do Windows e do email, a solução deve fornecer sugestões de mitigação genéricas em um painel dedicado na interface.

3.9.8.34.10. O banco de dados de mitigação como parte da solução deve incluir sugestões de mitigação para os seguintes fornecedores de soluções de segurança de rede:

- Cisco (funcionalidade de prevenção de intrusão de rede)
- Fortigate (prevenção de intrusão de rede e aplicação web)
- McAfee/Trellix (funcionalidade de prevenção de invasões de rede)
- ModSecurity(OpenSource)(firewall de aplicativo da web)
- Snort (código aberto) (prevenção de intrusão de rede)
- TrendMicro (prevenção de invasão de rede)

3.9.8.35. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as seguintes funcionalidades de Gerenciamento e Segurança:

3.9.8.35.1. A solução deve executar ataques cibernéticos sem implantar serviços vulneráveis.

3.9.8.35.2. A solução deve avaliar os controles Endpoint, Network e Email Security executados em sistemas físicos, virtuais e em nuvem, por meio de um agente unificado do Windows com suporte às versões Windows 7, 8.1, 10 e 11 do sistema operacional cliente e às versões 2012 R2, 2016, 2019 e 2022 do sistema operacional do servidor .

3.9.8.35.3. A solução deve avaliar os ataques de infiltração de rede nos sistemas operacionais MacOS 11 Big Sur e MacOS 12 Monterey executados em processadores baseados em Intel ou M1.

3.9.8.35.4. A solução deve avaliar ataques de infiltração de rede em sistemas operacionais baseados em Linux x86 e x64 (Redhat 7, Redhat 8, CentOS 7, CentOS 8).

3.9.8.35.5. Heartbeat – A solução deve verificar automaticamente os requisitos de conectividade entre seus componentes de ataque e relatar imediatamente quaisquer problemas de conectividade identificados antes de cada avaliação.

3.9.8.35.6. A proposta de solução deve permitir a configuração de cada agente para que sugestões de mitigação possam ser geradas de acordo com uma lista de tecnologias de fornecedores.

3.9.8.35.7. A solução deve ter pelo menos medidas de comunicação e autenticação criptografadas baseadas em certificado para proteger as comunicações entre seus componentes de software.

3.9.8.36. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as Serviços de Detecção e Analytics:

3.9.8.36.1. A solução deve ter a capacidade de analisar se as ameaças nos vetores de ataque testados são detectadas e alertadas nas soluções "Security Information and Event Management" (SIEM) e Endpoint Detection and Response (EDR), conectando-se à(s) plataforma(s) de solução relevante(s)).

3.9.8.36.2. Ao se conectar às soluções SIEM e EDR, a solução deve fornecer uma conexão via "API" usando autenticação de usuário-senha ou token.

3.9.8.36.3. Após a configuração da solução para integração com soluções SIEM ou EDR, ela deverá ser capaz de emitir um aviso em caso de problemas de acesso.

3.9.8.36.4. Ao configurar a conectividade com soluções de log relevantes para evitar falhas e validar os dados de log, a solução deve ter uma funcionalidade dedicada para testar automaticamente a precisão e a operação correta das consultas definidas pelo usuário.

3.9.8.36.5. A solução deve fornecer uma interface para determinar quando as consultas são feitas após o término dos ataques. (Tempo de atraso)

3.9.8.36.6. A solução deve fornecer uma interface para determinar um período de tempo para compensar pequenas diferenças de tempo entre os agentes e o servidor de gerenciamento. (horário inicial)

3.9.8.36.7. A solução deve fornecer uma interface para definir um limite de consultas simultâneas que podem ser feitas à solução SIEM/EDR para realizar análises de detecção de ameaças paralelas ao mesmo tempo.

3.9.8.36.8. A solução deve ter uma interface que possa mostrar a cobertura do framework MITRE ATT&CK de acordo com os resultados da detecção de ataques do cenário Windows Endpoint.

3.9.8.36.9. A solução deve relatar o número total de ameaças simuladas registradas, não registradas ou alertadas, não alertadas para cada simulação. Será fornecida uma lista de resultados de detecção para ameaças bloqueadas e não bloqueadas.

3.9.8.36.10. A solução deve oferecer suporte aos resultados da análise de detecção a serem exibidos de acordo com as categorias de ataque (Download de arquivo, Aplicações Web e Ataques de cenário de endpoint do Windows).

3.9.8.36.11. A solução deve fornecer uma interface para visualizar e comparar o status de detecção nos últimos 7/30/90 dias.

3.9.8.36.12. A solução deve ser capaz de mostrar o status de prevenção e detecção de qualquer ameaça simulada no mesmo painel de resultados da simulação.

3.9.8.36.13. A análise de detecção, a solução será capaz de mostrar o "horário de início" do ataque simulado, "o tempo de término", "o tempo entre dois períodos" e, além disso, o "tempo de registro", "o tempo entre final do ataque e registro", "o tempo entre o fim do ataque e a ocorrência do alerta".

3.9.8.36.14. A solução deve ser capaz de produzir no formato CSV com a finalidade de relatar ameaças detectadas ou não detectadas e deve ser capaz de mostrar se um alarme foi disparado após um ataque simulado ou não.

3.9.8.36.15. A solução deve ser capaz de gerar resultados de detecção de ameaças em um relatório PDF com ameaças registradas ou não registradas e ameaças alertadas ou não alertadas.

3.9.8.36.16. A solução deve possuir uma infraestrutura que verifique se os “dados de eventos” que ocorrem devido a cada simulação de ataque geram alertas.

3.9.8.36.17. Os resultados de alerta para os ataques de cenário de endpoint devem ser combinados com as técnicas e táticas da estrutura MITRE ATT&CK pela solução.

3.9.8.36.18. A solução deve validar os eventos ou logs recolhidos dos sistemas com os quais está integrada (nomeadamente soluções Log Management, SIEM ou EDR) para mostrar aqueles

eventos ou logs especificamente relacionados com cada ameaça simulada e apresentá-los ao utilizador.

3.9.8.36.19. A solução deve ser capaz de permitir que os usuários selecionem se desejam armazenar a saída bruta do log de detecção das fontes de dados.

3.9.8.36.20. Deve ser possível definir o armazenamento de logs.

3.9.8.36.21. Deve ser possível definir o número de entradas de logs registradas em cada simulação.

3.9.8.36.22. A solução a ser utilizada na prestação destes serviços deve atender a, no mínimo, as seguintes funcionalidades de Relatoria:

3.9.8.36.23. A solução deve relatar o número total de simulações de ataque executadas, juntamente com o número de ataques bloqueados e não bloqueados, para cada simulação. Uma lista de ataques totais bloqueados e não bloqueados será fornecida.

3.9.8.36.24. A solução deve ser capaz de exportar a lista de sugestões de mitigação específica do fornecedor com ID de assinatura, nome da assinatura, gravidade do fornecedor, contagem de ações não bloqueadas e informações de impacto de pontuação no formato CSV (valores separados por vírgula).

3.9.8.36.25. A solução deve fornecer uma interface gráfica para comparar as mudanças de status de segurança nos últimos 07/30/90 dias.

3.9.8.36.26. A solução deve permitir a geração de relatórios individuais de simulação para prevenção e detecção ou apenas para resultados de prevenção nos formatos CSV e PDF sob demanda.

3.9.9. SERVIÇOS DE CONTROLE E AUDITORIA DE ACESSOS

3.9.9.1. Todos os acessos do pessoal da CONTRATADA deverá ser realizado por meio de solução tecnológica que permita o controle e a auditoria dos acessos realizados aos ativos da PRODEB.

3.9.9.2. Os controles de acesso e registos de auditoria devem ser realizados tanto pelo pessoal que atue dentro das instalações da PRODEB como por aqueles que atuem remotamente.

3.9.9.3. A solução a ser utilizada deve possuir, no mínimo, as seguintes características para garantir a segurança dos acessos, além de visibilidade e gerenciamento das ações da CONTRATADA por parte da PRODEB:

3.9.9.4. Suportar o acesso externo a rede sem qualquer necessidade de utilização de VPN ou método similar de acesso;

3.9.9.5. Permitir o acesso remoto, no mínimo, aos seguintes sistemas operacionais:

3.9.9.5.1. Microsoft Windows 10 e superiores;

3.9.9.5.2. Servidores Windows Server 2012 e superiores;

3.9.9.5.3. Linux Red Hat Enterprise 6.0 e superiores.

3.9.9.6. Utilizar protocolos de comunicação fazendo uso de criptografia TLS 1.2 ou superior;

3.9.9.7. Suportar o funcionamento a redes que não estão conectadas diretamente a internet e a redes seguras;

3.9.9.8. Suportar o acesso sem necessidade de permissão prévia para o acesso a desktops e servidores;

3.9.9.9. Possibilitar o acesso a dispositivos de rede via SSH, como roteadores e switches;

3.9.9.10. Disponibilizar aos usuários, console de acesso Web para a solução, sem a necessidade de instalação de plug-ins ou agentes;

3.9.9.11. Suportar provedores externos de identidades para autenticação, incluindo, no mínimo, servidores LDAP, Active Directory, RADIUS e Kerberos, bem como atribuir privilégios com base na hierarquia e nas configurações de grupo já especificadas nos respectivos servidores;

3.9.9.12. Integrar-se com soluções de autenticação de duplo fator através de protocolo RADIUS, Single Sign-on via SAML ou OIDC e Time-Based One-Time Password (TOTP);

3.9.9.13. Permitir o agendamento para liberação do acesso remoto, incluindo notificação por e-mail aos destinatários designados;

3.9.9.14. Permitir forçar o encerramento da sessão remota pelo supervisor, com notificação ao cliente;

3.9.9.15. Prover monitoramento ao vivo e gravação da sessão, com registro completo das atividades executadas durante a sessão executada pelos usuários;

3.9.9.16. Limitar o acesso a aplicativos especificados no sistema remoto, incluindo a acesso a área de trabalho remota;

3.9.9.17. Suportar filtro de comandos durante as sessões SSH, visando evitar que o usuário inadvertidamente use um comando que pode causar danos ao servidor acessado;

3.9.9.18. Suportar a injeção automática de credenciais em sistemas Windows, permitindo que os usuários autentiquem ou elevem privilégios sem revelar credenciais, bem como a ação de "executar como";

3.9.9.19. Suportar a injeção automática de credenciais em sistemas Unix/Linux, permitindo que os usuários autentiquem ou elevem privilégios sem revelar credenciais, bem como a utilização em conjunto com o sudo;

3.9.9.20. Suportar o acesso com os seguintes modos:

3.9.9.20.1. Através de clientes instalados;

3.9.9.20.2. Através de agente de proxy local, que permite o acesso a sistemas autônomos em uma rede, sem cliente pré-instalado;

3.9.9.20.3. Acesso via agente de proxy local, que permite o acesso a sistemas em uma rede remota que não tenha uma conexão de internet nativa;

3.9.9.21. Suportar Remote Desktop Protocol (RDP), permitindo que os usuários colaborem em sessões auditadas e gravadas;

3.9.9.22. Permitir o monitoramento em tempo real das sessões de acesso feitas a ativos publicados na ferramenta;

3.9.9.23. Permitir a configuração de tempos limites para sessões ociosas, em que seja possível definir o tempo máximo para que um usuário inativo seja desconectado automaticamente;

3.9.9.24. Permitir que os usuários transfiram arquivos da máquina em que está conectado para o sistema remoto, através da console da solução e sem necessidade de uso de ferramentas de terceiros;

3.9.9.25. Permitir que os usuários compartilhem sessões de acesso com outros usuários do sistema, permitindo que os administradores colaborem em uma mesma sessão. Esta colaboração deve ser possível com usuários internos e externos através de convite;

3.9.9.26. Contar com proxy de banco de dados, para injetar credenciais e ter rastreabilidade total de comandos

3.9.9.27. A solução deve possuir integração com soluções de ITSM

3.9.9.28. A solução deve prover autenticação via Kerberos

3.9.10. REQUISITOS DE EQUIPE E CAPACITAÇÃO TÉCNICA DE ANALISTAS LOCADOS PARA PRODEB

3.9.10.1. Deverá conter no mínimo 2 (dois) profissionais que serão considerados como prepostos da CONTRATADA, com perfil de Analista de Segurança, sendo 1 (um) com perfil de Analista de Segurança Pleno (3 a 5 anos de experiência em Segurança da Informação) e 1 (um) com perfil de Analista de Segurança Sênior (mais de 5 anos de experiência em Segurança da Informação).

3.9.10.2. Todos deverão ter experiência comprovada na operação, configuração, administração de soluções de segurança, monitoramento e resposta a incidentes em segurança da informação;

3.9.10.3. Deverão ter graduação em cursos de tecnologia da informação, engenharia de computação e/ou pós-graduação em segurança da informação;

3.9.10.4. Estes profissionais deverão executar suas atividades presencialmente na PRODEB em regime mínimo de 8x5.

3.9.10.5. A equipe deverá possuir, somados, no mínimo, 3 (três) das certificações técnicas abaixo listadas:

3.9.10.5.1. Certified Information Security Manager (CISM).

3.9.10.5.2. Certified Information Systems Security Professional (CISSP).

3.9.10.5.3. EC-Council Certified Ethical Hacker Master.

3.9.10.5.4. EC-Council Certified Ethical Hacker Practical.

3.9.10.5.5. CompTIA Security +.

3.9.10.5.6. CompTIA CySA+.

3.9.10.5.7. CompTIA CASP+.

3.9.10.5.8. EC-Council Certified SOC Analyst (CSA).

3.9.10.5.9. EC-Council Certified Incident Handler (E|CIH).

3.9.10.5.10. GIAC Certified Incident Handler (GCIH).

3.9.10.5.11. GIAC Continuous Monitoring Certification (GMON).

3.9.10.5.12. EXIN ISFS Foundation.

3.9.10.5.13. Linux Professional LPIC.

3.9.10.5.14. Vulnerability Management Foundation.

3.9.10.5.15. ISO/IEC 27001:2013 Foundation (I27001F).

3.9.10.5.16. ICSI | Certified Network Security Specialist (CNSS).

3.9.10.5.17. Scrum Foundation Professional Certificate

3.9.10.5.18. ITIL Foundation

3.9.10.5.19. COBIT Foundation

3.9.10.5.20. CompTIA Advanced Security Practitioner (CASP+)

3.9.10.5.21. Cybersecurity Professional Certificate – LCSPC by CyBok.

3.9.11. REQUISITOS DE EQUIPE E CAPACITAÇÃO TÉCNICA DE ANALISTAS REMOTOS

3.9.11.1. A CONTRATADA deverá alocar quantos profissionais sejam necessários, mesmo que remotamente, para entregar os serviços ora contratados dentro dos Níveis de Serviço estabelecidos na seção Acordo de Nível de Serviços - ANS.

3.9.11.2. A equipe de plantão, deverá ser integrada por turno de trabalho em no mínimo, 2 (dois) profissionais, sendo ao menos 1 (um) profissional com o perfil de Analista de Segurança Sênior.

3.9.11.3. O conjunto da equipe alocada pela CONTRATADA deverá comprovar as certificações técnicas dos fabricantes de todas as soluçõesconstante no ANEXO III – SOLUÇÕES DE SEGURANÇA além das certificações conforme requisito constante no item 5.9.10.5;

3.9.11.4. A CONTRATADA deve garantir que no mesmo turno de trabalho, haja profissionais capacitados para prestar os serviços estabelecidos neste Termo de Referência;

3.9.12. INDICADORES DE PERFORMANCE

3.9.12.1. A frequência de aferição dos indicadores de performance será mensal, porém com registros diários quando aplicável, devendo a contratada elaborar Relatório Mensal de Atividades, apresentando-o a CONTRATANTE até o quinto dia útil do mês subsequente ao da prestação do serviço.

3.9.12.2. Devem constar desse relatório, entre outras informações, as vulnerabilidades encontradas com as respectivas correções/mitigações sugeridas, riscos, ameaças, alertas, incidentes, indicadores de performance, metas de níveis de serviço alcançados, recomendações técnicas, administrativas e gerenciais para o próximo período e demais informações relevantes para a gestão contratual. O conteúdo detalhado e a forma do relatório gerencial serão definidos pelas partes.

3.9.12.3. Caberá à Equipe de Segurança da CONTRATANTE analisar o Relatório Mensal de Atividades executados pela Contratada, observando os indicadore e os níveis de serviço alcançados;

3.10. ITEM 10 - SERVIÇOS PROFISSIONAIS DE MONITORAMENTO E SEGURANÇA PARA O ITEM "SOLUÇÃO DE SEGURANÇA DE ENDPOINT - EPP" PARA CADA ITEM MONITORADO PELO PERÍODO DE 24 MESES

3.10.1. A CONTRATADA deverá prestar serviços de configuração, administração, operação, atendimento a mudanças e requisições, aplicação de melhores práticas do fabricante e monitoramento para a solução de Endpoint Protection especificada no item "Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Endpoint - EPP" para cada item monitorado pelo período de 24 Meses." deste Termo de Referência, conforme as necessidades da CONTRATANTE;

3.10.2. O serviço deverá ser iniciado após a emissão da Ordem de Serviço, a ser enviada pela CONTRATANTE, após a entrega do Termo de Homologação de instalação do item "Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Endpoint - EPP" para cada item monitorado pelo período de 24 Meses.";

3.10.3. Os serviços serão pagos mensalmente, de acordo com o volume de dispositivos a serem monitorados pela CONTRATADA.

3.10.4. A CONTRATADA será responsável por projetar, instalar, configurar, gerenciar e monitorar a solução ofertada;

3.10.5. A CONTRATADA, em até 05 (cinco) dias, após a emissão da Ordem de Serviço por parte da CONTRATANTE, deverá elaborar um projeto de implantação contendo gerenciamento de escopo, risco, mudanças, cronograma de instalação, gerenciamento de recursos humanos, contendo planejamento detalhado para permitir uma instalação com o menor risco de impacto possível, detalhando o passo a passo dos serviços;

3.10.6. A CONTRATADA deverá cumprir com todas as exigências técnicas e funcionais relacionadas com a solução ofertada, que devem ser implantadas durante o período contratado, sem ônus para a CONTRATANTE;

3.10.7. O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares estritamente necessários à implantação e suporte é de inteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;

3.10.8. No processo de implantação o Responsável Técnico deverá tomar todas as medidas necessárias visando garantir a perfeita execução do serviço (instalação e configuração);

3.10.9. No prazo de até 10 (dez) dias após a conclusão da ativação do serviço, a CONTRATADA deverá fornecer documentação final contendo as orientações para acionamento do serviço, papeis e responsabilidades, acesso ao sistema de gerenciamento de chamados, acesso ao Painel de Gestão para acompanhamento, e todas as informações relevantes para a plena utilização do serviço por parte da CONTRATANTE;

3.10.10. A documentação deverá ser aprovada pela CONTRATANTE e pelo GESTOR TÉCNICO, caracterizando a homologação da solução em um prazo de até 10 dias úteis, quando a CONTRATANTE emitirá um Termo de Homologação;

3.10.11. Caso seja identificado defeito ou falha sistemática em determinado produto/serviço entregue pela CONTRATADA, ou ainda, que nos testes realizados sejam considerados em desacordo com as especificações

técnicas requeridas, o Gestor Técnico e a CONTRATANTE podem exigir a substituição, total ou parcial, do referido produto;

3.10.12. A CONTRATADA será responsável pelo monitoramento da solução em regime 24x7x365, devendo manter a mesma sempre atualizada e em operação;

3.10.13. Deve ser elaborado e enviado mensalmente um relatório executivo com o resumo das principais ocorrências e as providências executadas pela CONTRATADA, além de gráficos e estatísticas relativos à conformidade operacional do ambiente. A formatação deste relatório deve estar em comum acordo com a CONTRATANTE;

3.10.14. A manutenção visa manter em perfeito estado de operação os serviços fornecidos em atendimento ao objeto, deste modo a CONTRATADA deve cumprir os seguintes procedimentos:

3.10.14.1. Desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

3.10.14.2. Quanto às atualizações pertinentes aos softwares, entende-se como "atualização" o provimento de toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas releases, versions, builds, upgrades, englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado;

3.10.15. A CONTRATADA deverá monitorar índice de atualização do conteúdo de segurança (ex: assinaturas) e engines/motores de detecção alertando quando índice de atualizações das máquinas estiver abaixo de 90%;

3.10.16. A operação e administração da solução será realizada pela CONTRATADA conforme as orientações e solicitações de configurações e políticas realizadas pelo Gestor Técnico da CONTRATANTE;

3.10.17. As solicitações de alteração de configurações deverão ser realizadas conforme o ANS definido na Seção – Acordo de Nível de Serviço – ANS;

3.10.18. No caso de necessidade de ações preventivas ou corretivas a CONTRATADA agendará com antecedência junto a CONTRATANTE as implementações das correções, fora do horário comercial, preferencialmente em feriados e finais de semana. Nenhuma ação poderá ser executada no ambiente sem a ciência e anuência do CONTRATANTE;

3.10.19. A CONTRATADA deverá prestar suporte aos componentes de software fornecidos para a implementação e utilização da solução;

3.10.20. A CONTRATADA deverá disponibilizar serviço de suporte técnico e manutenção, no regime (24x7x365) vinte e quatro horas por dia, sete dias por semana, pelo período da contratação;

3.10.21. Os acionamentos dos serviços de suporte e manutenção serão requisitados por meio de ordens de serviço, a serem abertas pelo CONTRATANTE, através de número de telefone nacional (0800 com serviço de uso ilimitado) disponibilizado pela CONTRATADA, e ainda, por e-mail e sítio de internet;

3.10.22. Não haverá limitação no número de chamados que poderão ser abertos;

3.10.23. A CONTRATADA manterá registro de todas as ordens de serviço abertas, disponibilizando, para cada uma, no mínimo as seguintes informações:

3.10.23.1. Número sequencial da ordem;

3.10.23.2. Data e hora de abertura;

3.10.23.3. Severidade;

3.10.23.4. Descrição do problema;

3.10.23.5. Data e hora do início do atendimento;

3.10.23.6. Data e hora de término do atendimento (solução).

3.10.24. O serviço de suporte técnico e manutenção deverá ser prestado por profissional devidamente certificado nas soluções tecnológicas utilizadas na prestação dos serviços contratados;

3.10.25. As informações relacionadas à ANS estão na Seção – Acordo de Nível de Serviço – ANS.

3.11. ITEM 11 - SERVIÇOS PROFISSIONAIS DE MONITORAMENTO E SEGURANÇA PARA O ITEM "SOLUÇÃO PARA DUPLO FATOR DE AUTENTICAÇÃO - TOKEN MOBILE" PARA CADA ITEM MONITORADO PELO PERÍODO DE 24 MESES.

3.11.1. A CONTRATADA deverá prestar serviços de configuração, administração, operação, atendimento a mudanças e requisições, aplicação de melhores práticas do fabricante, para a solução de duplo fator de autenticação especificada no item "serviços profissionais de monitoramento e segurança para o item "solução para duplo fator de autenticação - token mobile" para cada item monitorado pelo período de 24 meses" deste Termo de Referência, conforme as necessidades da CONTRATANTE.

3.11.2. O serviço deverá ser iniciado após a emissão da Ordem de Serviço, a ser enviada pela CONTRATANTE, após a entrega do Termo de Homologação de instalação do item "SERVIÇOS PROFISSIONAIS DE

MONITORAMENTO E SEGURANÇA PARA O ITEM "SOLUÇÃO PARA DUPLO FATOR DE AUTENTICAÇÃO - TOKEN MOBILE" PARA CADA ITEM MONITORADO PELO PERÍODO DE 24 MESES";

3.11.3. Os serviços serão pagos mensalmente, de acordo com o volume de dispositivos a serem monitorados pela CONTRATADA.

3.11.4. A CONTRATADA será responsável por projetar, instalar, configurar, gerenciar e monitorar a solução ofertada;

3.11.5. A CONTRATADA, em até 05 (cinco) dias, após a emissão da Ordem de Serviço por parte da CONTRATANTE, deverá elaborar um projeto de implantação contendo gerenciamento de escopo, risco, mudanças, cronograma de instalação, gerenciamento de recursos humanos, contendo planejamento detalhado para permitir uma instalação com o menor risco de impacto possível, detalhando o passo a passo dos serviços;

3.11.6. A CONTRATADA deverá cumprir com todas as exigências técnicas e funcionais relacionadas com a solução ofertada, que devem ser implantadas durante o período contratado, sem ônus para a CONTRATANTE;

3.11.7. O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares estritamente necessários à instalação ou à assistência técnica é de inteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;

3.11.8. No processo de instalação o Responsável Técnico deverá tomar todas as medidas necessárias visando garantir a perfeita execução do serviço (instalação e configuração);

3.11.9. A solução de segurança deverá ser integrada ao core da solução de autenticação do Data Center da PRODEB, sendo essa configuração realizada pela CONTRATADA com base nas informações fornecidas pela PRODEB;

3.11.10. No prazo de até 10 (dez) dias após a conclusão da ativação do serviço, a CONTRATADA deverá fornecer documentação final contendo as orientações para acionamento do serviço, papeis e responsabilidades, acesso ao sistema de gerenciamento de chamados, acesso ao Painel de Gestão para acompanhamento, e todas as informações relevantes para a plena utilização do serviço por parte da CONTRATANTE;

3.11.11. A documentação deverá ser aprovada pela CONTRATANTE e pelo GESTOR TÉCNICO, caracterizando a homologação da solução em um prazo de até 10 dias úteis, quando a CONTRATANTE emitirá um Termo de Homologação;

3.11.12. Caso seja identificado defeito ou falha sistemática em determinado produto/serviço entregue pela CONTRATADA, ou ainda, que nos testes realizados sejam considerados em desacordo com as especificações técnicas requeridas, o Gestor Técnico e a CONTRATANTE podem exigir a substituição, total ou parcial, do referido produto;

3.11.13. Deve ser elaborado e enviado mensalmente um relatório executivo com o resumo das principais ocorrências e as providências executadas pela CONTRATADA, além de gráficos e estatísticas relativos à conformidade operacional do ambiente. A formatação deste relatório deve estar em comum acordo com a CONTRATANTE;

3.11.14. A manutenção visa manter em perfeito estado de operação os serviços fornecidos em atendimento ao

3.11.15. As solicitações de alteração de configurações deverão ser realizadas conforme o ANS definido na Seção – Acordo de Nível de Serviço – ANS;

3.11.16. No caso de necessidade de ações preventivas ou corretivas a CONTRATADA agendará com antecedência junto a CONTRATANTE as implementações das correções, fora do horário comercial, preferencialmente em feriados e finais de semana. Nenhuma ação poderá ser executada no ambiente sem a ciência e anuência do CONTRATANTE;

3.11.17. A CONTRATADA deverá prestar suporte a todos os componentes de software fornecidos para a implementação e utilização da solução;

3.11.18. A CONTRATADA deverá disponibilizar serviço de suporte técnico e manutenção, no regime (24x7x365) vinte e quatro horas por dia, sete dias por semana, pelo período da contratação;

3.11.19. Os acionamentos dos serviços de suporte e manutenção serão requisitados por meio de ordens de serviço, a serem abertas pelo CONTRATANTE, através de número de telefone nacional (0800 com serviço de uso ilimitado) disponibilizado pela CONTRATADA, e ainda, por e-mail e sítio de internet;

3.11.20. Não haverá limitação no número de chamados que poderão ser abertos;

3.11.21. A CONTRATADA manterá registro de todas as ordens de serviço abertas, disponibilizando, para cada uma, no mínimo as seguintes informações:

- 3.11.21.1. Número sequencial da ordem;
- 3.11.21.2. Data e hora de abertura;
- 3.11.21.3. Severidade;
- 3.11.21.4. Descrição do problema;
- 3.11.21.5. Data e hora do início do atendimento;
- 3.11.21.6. Data e hora de término do atendimento (solução).

3.11.22. O serviço de suporte técnico e manutenção deverá ser prestado por profissional devidamente certificado nas soluções tecnológicas utilizadas na prestação dos serviços contratados;

3.11.23. As informações relacionadas à ANS estão na Seção – Acordo de Nível de Serviço – ANS.

3.12. ITEM 12 - SERVIÇOS PROFISSIONAIS DE MONITORAMENTO E SEGURANÇA PARA OS ITENS "SOLUÇÃO DE SEGURANÇA DE REDE NGFW TIPO I, II" PARA CADA ITEM MONITORADO PELO PERÍODO DE 24 MESES.

3.12.1. A CONTRATADA deverá prestar serviços de configuração, administração, operação, atendimento a mudanças e requisições, aplicação de melhores práticas do fabricante, monitoramento e resposta a incidentes para a solução de ngfw especificada nos itens "solução de segurança de rede ngfw tipo i, ii" deste Termo de Referência, conforme as necessidades da CONTRATANTE.

3.12.2. O serviço deverá ser iniciado após a emissão da Ordem de Serviço, a ser enviada pela CONTRATANTE, após a entrega do Termo de Homologação de instalação dos itens "SOLUÇÃO DE SEGURANÇA DE REDE NGFW TIPO I, II;

3.12.3. Os serviços serão pagos mensalmente, de acordo com o volume de dispositivos a serem monitorados pela CONTRATADA.

3.12.4. A UNIDADE de contratação para prestação destes serviços mensais aplica-se a cada unidade de dispositivo a ser monitorado pela CONTRATADA.

3.12.5. A CONTRATADA será responsável por projetar, instalar, configurar, gerenciar e monitorar a solução ofertada;

3.12.6. A CONTRATADA, em até 05 (cinco) dias, após a emissão da Ordem de Serviço por parte da CONTRATANTE, deverá elaborar um projeto de implantação contendo gerenciamento de escopo, risco, mudanças, cronograma de instalação, gerenciamento de recursos humanos, contendo planejamento detalhado para permitir uma instalação com o menor risco de impacto possível, detalhando o passo a passo dos serviços;

3.12.7. A CONTRATADA deverá cumprir com todas as exigências técnicas e funcionais relacionadas com a solução ofertada, que devem ser implantadas durante o período contratado, sem ônus para a CONTRATANTE;

3.12.8. O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares estritamente necessários à instalação ou à assistência técnica é de inteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;

3.12.9. No processo de instalação o Responsável Técnico deverá tomar todas as medidas necessárias visando garantir a perfeita execução do serviço (instalação e configuração);

3.12.10. A solução de segurança deverá ser integrada ao core da solução de autenticação do Data Center da PRODEB, sendo essa configuração realizada pela CONTRATADA com base nas informações fornecidas pela PRODEB;

3.12.11. No prazo de até 10 (dez) dias após a conclusão da ativação do serviço, a CONTRATADA deverá fornecer documentação final contendo as orientações para acionamento do serviço, papeis e responsabilidades, acesso ao sistema de gerenciamento de chamados, acesso ao Painel de Gestão para acompanhamento, e todas as informações relevantes para a plena utilização do serviço por parte da CONTRATANTE;

3.12.12. A documentação deverá ser aprovada pela CONTRATANTE e pelo GESTOR TÉCNICO, caracterizando a homologação da solução em um prazo de até 10 (dez) dias úteis, quando a CONTRATANTE emitirá um Termo de Homologação;

3.12.13. Caso seja identificado defeito ou falha sistemática em determinado produto/serviço entregue pela CONTRATADA, ou ainda, que nos testes realizados sejam considerados em desacordo com as especificações técnicas requeridas, o Gestor Técnico e a CONTRATANTE podem exigir a substituição, total ou parcial, do referido produto;

3.12.14. A CONTRATADA será responsável pelo monitoramento da solução em regime 24x7x365, devendo manter a mesma sempre atualizada e em operação;

3.12.15. Deve ser elaborado e enviado mensalmente um relatório executivo com o resumo das principais ocorrências e as providências executadas pela CONTRATADA, além de gráficos e estatísticas relativos à conformidade operacional do ambiente. A formatação deste relatório deve estar em comum acordo com a CONTRATANTE;

3.12.16. A manutenção visa manter em perfeito estado de operação os serviços fornecidos em atendimento ao objeto, deste modo a CONTRATADA deve cumprir os seguintes procedimentos:

3.12.17. Desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

3.12.18. Quanto às atualizações pertinentes aos softwares, entende-se como "atualização" o provimento de toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas releases,

versions, builds, upgrades, englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado;

3.12.19. A operação e administração (gerenciamento total) da solução será realizada pela CONTRATADA conforme as orientações e solicitações de configurações e políticas realizadas pelo Gestor Técnico da CONTRATANTE;

3.12.20. As solicitações de alteração de configurações deverão ser realizadas conforme o ANS definido na Seção – Acordo de Nível de Serviço – ANS;

3.12.21. No caso de necessidade de ações preventivas ou corretivas a CONTRATADA agendará com antecedência junto a CONTRATANTE as implementações das correções, fora do horário comercial, preferencialmente em feriados e finais de semana. Nenhuma ação poderá ser executada no ambiente sem a ciência e anuência do CONTRATANTE;

3.12.22. A CONTRATADA deverá prestar suporte a todos os componentes de software fornecidos para a implementação e utilização da solução;

3.12.23. A CONTRATADA deverá disponibilizar serviço de suporte técnico e manutenção, no regime (24x7x365) vinte e quatro horas por dia, sete dias por semana, pelo período da contratação;

3.12.24. Os acionamentos dos serviços de suporte e manutenção serão requisitados por meio de ordens de serviço, a serem abertas pelo CONTRATANTE, através de número de telefone nacional (0800 com serviço de uso ilimitado) disponibilizado pela CONTRATADA, e ainda, por e-mail e sítio de internet;

3.12.25. Não haverá limitação no número de chamados que poderão ser abertos;

3.12.26. A CONTRATADA manterá registro de todas as ordens de serviço abertas, disponibilizando, para cada uma, no mínimo as seguintes informações:

- 3.12.26.1. Número sequencial da ordem;
- 3.12.26.2. Data e hora de abertura;
- 3.12.26.3. Severidade;
- 3.12.26.4. Descrição do problema;
- 3.12.26.5. Data e hora do início do atendimento;
- 3.12.26.6. Data e hora de término do atendimento (solução).

3.12.27. O serviço de suporte técnico e manutenção deverá ser prestado por profissional devidamente certificado nas soluções tecnológicas utilizadas na prestação dos serviços contratados;

3.12.28. As informações relacionadas à ANS estão na Seção – Acordo de Nível de Serviço – ANS.

3.13. ITEM 13 - SERVIÇOS PROFISSIONAIS DE MONITORAMENTO E SEGURANÇA PARA O ITEM "SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAF TIPO I" PARA CADA ITEM MONITORADO PELO PERÍODO DE 24 MESES.

3.13.1. A CONTRATADA deverá prestar serviços de configuração, administração, operação, atendimento a mudanças e requisições, aplicação de melhores práticas do fabricante, monitoramento e resposta a incidentes para a solução de WAF (Web Application Fiewall) especificada no item "SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAF TIPO I" deste Termo de Referência, conforme as necessidades da CONTRATANTE.

3.13.2. O serviço deverá ser iniciado após a emissão da Ordem de Serviço, a ser enviada pela CONTRATANTE, após a entrega do Termo de Homologação de instalação do item "SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAF TIPO I";

3.13.3. Os serviços serão pagos mensalmente, de acordo com o volume de dispositivos a serem monitorados pela CONTRATADA.

3.13.4. A UNIDADE de contratação para prestação destes serviços mensais aplica-se a cada dispositivo a ser monitorado pela CONTRATADA.

3.13.5. A CONTRATADA será responsável por projetar, instalar, configurar, gerenciar e monitorar a solução ofertada;

3.13.6. A CONTRATADA, em até 05 (cinco) dias, após a emissão da Ordem de Serviço por parte da CONTRATANTE, deverá elaborar um projeto de implantação contendo gerenciamento de escopo, risco, mudanças, cronograma de instalação, gerenciamento de recursos humanos, contendo planejamento detalhado para permitir uma instalação com o menor risco de impacto possível, detalhando o passo a passo dos serviços;

3.13.7. A CONTRATADA deverá cumprir com todas as exigências técnicas e funcionais relacionadas com a solução ofertada, que devem ser implantadas durante o período contratado, sem ônus para a CONTRATANTE;

3.13.8. O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares estritamente necessários à instalação ou à assistência técnica é de inteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;

3.13.9. No processo de instalação o Responsável Técnico deverá tomar todas as medidas necessárias visando garantir a perfeita execução do serviço (instalação e configuração);

3.13.10. No prazo de até 10 (dez) dias após a conclusão da ativação do serviço, a CONTRATADA deverá fornecer documentação final contendo as orientações para acionamento do serviço, papeis e responsabilidades, acesso ao sistema de gerenciamento de chamados, acesso ao Painel de Gestão para acompanhamento, e todas as informações relevantes para a plena utilização do serviço por parte da CONTRATANTE;

3.13.11. A documentação deverá ser aprovada pela CONTRATANTE e pelo GESTOR TÉCNICO, caracterizando a homologação da solução em um prazo de até 10 dias úteis, quando a CONTRATANTE emitirá um Termo de Homologação;

3.13.12. Caso seja identificado defeito ou falha sistemática em determinado produto/serviço entregue pela CONTRATADA, ou ainda, que nos testes realizados sejam considerados em desacordo com as especificações técnicas requeridas, o Gestor Técnico e a CONTRATANTE podem exigir a substituição, total ou parcial, do referido produto;

3.13.13. A CONTRATADA será responsável pelo monitoramento da solução em regime 24x7x365, devendo manter a mesma sempre atualizada e em operação;

3.13.14. Deve ser elaborado e enviado mensalmente um relatório executivo com o resumo das principais ocorrências e as providências executadas pela CONTRATADA, além de gráficos e estatísticas relativos à conformidade operacional do ambiente. A formatação deste relatório deve estar em comum acordo com a CONTRATANTE;

3.13.15. A manutenção visa manter em perfeito estado de operação os serviços fornecidos em atendimento ao objeto, deste modo a CONTRATADA deve cumprir os seguintes procedimentos:

3.13.16. Desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

3.13.17. Quanto às atualizações pertinentes aos softwares, entende-se como "atualização" o provimento de toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas releases, versions, builds, upgrades, englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia especificado;

3.13.18. A operação e administração (gerenciamento total) da solução será realizada pela CONTRATADA conforme as orientações e solicitações de configurações e políticas realizadas pelo Gestor Técnico da CONTRATANTE;

3.13.19. As solicitações de alteração de configurações deverão ser realizadas conforme o ANS definido na Seção – Acordo de Nível de Serviço – ANS;

3.13.20. No caso de necessidade de ações preventivas ou corretivas a CONTRATADA agendará com antecedência junto a CONTRATANTE as implementações das correções, fora do horário comercial, preferencialmente em feriados e finais de semana. Nenhuma ação poderá ser executada no ambiente sem a ciência e anuência do CONTRATANTE;

3.13.21. A CONTRATADA deverá prestar suporte a todos os componentes de software fornecidos para a implementação e utilização da solução;

3.13.22. A CONTRATADA deverá disponibilizar serviço de suporte técnico e manutenção, no regime (24x7x365) vinte e quatro horas por dia, sete dias por semana, pelo período da contratação;

3.13.23. Os acionamentos dos serviços de suporte e manutenção serão requisitados por meio de ordens de serviço, a serem abertas pelo CONTRATANTE, através de número de telefone nacional (0800 com serviço de uso ilimitado) disponibilizado pela CONTRATADA, e ainda, por e-mail e sítio de internet;

3.13.24. Não haverá limitação no número de chamados que poderão ser abertos;

3.13.25. A CONTRATADA manterá registro de todas as ordens de serviço abertas, disponibilizando, para cada uma, no mínimo as seguintes informações:

- 3.13.25.1. Número sequencial da ordem;
- 3.13.25.2. Data e hora de abertura;
- 3.13.25.3. Severidade;
- 3.13.25.4. Descrição do problema;
- 3.13.25.5. Data e hora do início do atendimento;
- 3.13.25.6. Data e hora de término do atendimento (solução).

3.13.26. O serviço de suporte técnico e manutenção deverá ser prestado por profissional devidamente certificado nas soluções tecnológicas utilizadas na prestação dos serviços contratados;

3.13.27. As informações relacionadas à ANS estão na Seção – Acordo de Nível de Serviço – ANS.

IV. OBRIGAÇÕES ESPECÍFICAS DA CONTRATAÇÃO

4. DA INSTALAÇÃO E HOMOLOGAÇÃO:

4.1. **INSTALAÇÃO E HOMOLOGAÇÃO DOS ITENS 01, 02, 03, 04, 05**

4.1.1. Em até 10 (dez) dias úteis 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;

4.1.2. A Instalação dos equipamentos e softwares deverá iniciar em até 15 (quinze) dias após o recebimento definitivo, podendo este prazo ser prorrogado em caso de necessidade da PRODEB, hipótese em que a CONTRATADA deverá ser formal e justificadamente comunicada;

4.1.3. Durante a instalação, os profissionais da CONTRATADA deverão informar todas as ações executadas para os profissionais indicados pela CONTRATANTE;

4.1.4. Entende-se por instalação dos equipamentos: a montagem física e acessórios fornecidos, bem como a configuração lógica de todos os equipamentos e softwares envolvidos;

4.1.5. Entende-se por instalação dos softwares a disponibilização em pleno funcionamento, configurado e licenciado pelo prazo especificado no respectivo item do Termo de Referência;

4.1.6. Deverão ser fornecidos pela CONTRATADA, quanto a instalação física, todos os cabos e conectores necessários, refefernetes aos itens 01 a 08, bem como os parafusos, porcas-gaiola, organizadores e demais acessórios necessários para montagem apropriada dos equipamentos no rack da CONTRATANTE;

4.1.7. Os serviços de instalação, configuração e migração poderão ser executados pela CONTRATADA fora do horário comercial, sábado ou domingo, cabendo a CONTRATANTE informar antecipadamente a CONTRATADA;

4.1.8. 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;

4.1.9. Será apresentado o ambiente atual da CONTRATANTE, onde a CONTRATADA deverá levantar todos os requisitos e configurações pertinentes à referida implantação;

4.1.10. Será apresentado pela CONTRATADA o Plano de Instalação, contemplando o que será migrado, as funcionalidades que serão implementadas segundo o Termo de Referência;

4.1.11. O Plano de Instalação poderá ser recusado pela CONTRATANTE, devendo a CONTRATADA realizar os ajustes definidos em reunião e reapresentá-los;

4.1.12. 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;

4.1.13. Concluído o serviço de instalação e os testes, no prazo de até 10 dias, a CONTRATADA deverá elaborar a respectiva documentação, contendo todas as informações da implantação: aspectos de arquitetura, configuração, descrição das características e recursos utilizados, testes, integrações;

4.1.14. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter nome, data e assinatura do técnico responsável da CONTRATADA;

4.1.15. A documentação deverá ser entregue em meio digital (formatos PDF e DOCx);

4.1.16. A documentação deverá ser validada pela equipe técnica da CONTRATANTE, devendo ser ajustada pela CONTRATADA caso seja solicitado.

4.1.17. Todos os serviços dos itens, devem ocorrer de maneira remota ou local, quando necessário, no Estado da Bahia.

4.1.18. No prazo de até 10 (dez) dias 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;

4.1.19. 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;

4.1.20. 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 identificas;

4.1.21. São condições para a assinatura do Termo de Homologação do Serviço por parte da CONTRATANTE:

4.1.21.1. A CONTRATANTE receber o comunicado da CONTRATADA informando da conclusão dos serviços de instalação, conforme descrito neste Termo de Referência;

4.1.21.2. A CONTRATANTE concluir a avaliação técnica qualitativa conforme condições constantes neste Termo de Referência e constatar que não existem inconformidades na solução instalada;

4.1.22. A CONTRATANTE receber toda documentação atualizada que contempla:

4.1.22.1. Visão geral da arquitetura da solução implantada, com desenho da estrutura lógica e física adotada quando necessário;

4.1.22.2. Descrição das etapas do processo de instalação, detalhando as opções de configuração adotadas;

4.1.22.3. Descrição do funcionamento das soluções, incluindo manuais de utilização dos portais web para visibilidade, para procedimento de abertura de chamado junto a CONTRATADA.

4.2. **INSTALAÇÃO E HOMOLOGAÇÃO DOS ITENS 06, 07, 08 no DATACENTER da PRODEB**

4.2.1. A CONTRATADA em até 10 (dez) úteis dias após a assinatura do contrato, deverá iniciar o planejamento para elaboração do Cronograma de Instalação dos equipamentos e soluções, em conjunto com a CONTRATANTE;

4.2.2. Durante a instalação, os profissionais da CONTRATADA deverão informar todas as ações executadas para os profissionais indicados pela CONTRATANTE;

4.2.3. Num prazo de até 10 (dez) dias após a conclusão de instalação da solução ofertada, a contratada deverá fornecer documentação final contendo os diagramas, as configurações e topologias de como foram instalados os equipamentos. A documentação deverá ser aprovada pela contratante, caracterizando a conclusão dos serviços;

4.2.4. O serviço de instalação e configuração dos itens, devem ocorrer na sede da CONTRATANTE, situada na Avenida 4, nº 410, Centro Administrativo da Bahia – CAB, Salvador, Bahia, CEP: 41.745-002;

4.2.5. Será apresentado pela CONTRATADA Projeto Executivo: Elaboração de projeto prévio para a implantação da solução conforme parâmetros do Termo de Referência.

4.2.6. O Plano de Instalação da solução poderá ser recusado pela CONTRATANTE, devendo a CONTRATADA realizar os ajustes definidos em reunião e reapresentá-los;

4.2.7. A CONTRATADA, depois de concluído o serviço de instalação da solução, deverá realizar, com acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para validar que a solução foi instalada de acordo com o Plano de Instalação;

4.2.8. Concluído o serviço de instalação e os testes, a CONTRATADA deverá elaborar a documentação da solução, contendo todas as informações da implantação, como aspectos de arquitetura, configuração, descrição das características e recursos utilizados, testes, integrações e etc.;

4.2.9. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter nome, data e assinatura do técnico responsável da CONTRATADA;

4.2.10. A documentação deverá ser entregue em em meio digital (formatos PDF e DOCx);

4.2.11. A documentação deverá ser validada pela equipe técnica da CONTRATANTE, devendo ser ajustada pela CONTRATADA caso seja solicitado.

4.2.12. No prazo de até 10 (dez) dias 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;

4.2.13. 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;

4.2.14. 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 identificas;

4.2.15. São condições para a assinatura do Termo de Homologação do Serviço por parte da CONTRATANTE:

4.2.15.1. A CONTRATANTE receber o comunicado da CONTRATADA informando da conclusão dos serviços de instalação, conforme descrito neste Termo de Referência;

4.2.15.2. A CONTRATANTE concluir a avaliação técnica qualitativa conforme condições constantes neste Termo de Referência e constatar que não existem inconformidades na solução instalada;

4.2.16. A CONTRATANTE receber toda documentação atualizada que contempla:

4.2.16.1. Visão geral da arquitetura da solução implantada, com desenho da estrutura lógica e física adotada quando necessário;

4.2.16.2. Descrição das etapas do processo de instalação, detalhando as opções de configuração adotadas;

4.2.16.3. Descrição do funcionamento das soluções, incluindo manuais de utilização dos portais web para visibilidade, para procedimento de abertura de chamado junto a CONTRATADA.

4.3. IMPLANTAÇÃO E HOMOLOGAÇÃO DOS SERVIÇOS DO ITEM 09

4.3.1. Em até 10 (dez) dias úteis após a emissão da Ordem de Serviço pela CONTRATANTE, deverá ser realizada uma reunião de alinhamento entre a CONTRATANTE e CONTRATADA, para detalhamento do Plano de Implantação;

4.3.2. No prazo de até 30 (trinta) dias após a emissão da Ordem de Serviço, a CONTRATADA deverá realizar avaliação completa do ambiente do CONTRATANTE com o objetivo identificar lacunas ou oportunidades de melhoria (Gap Analysis) com o objetivo de avaliar a maturidade dos controles de segurança do CONTRATANTE;

4.3.3. A CONTRATADA deverá realizar toda a instalação dos produtos que forem necessários, incluindo a configuração: dos produtos instalados, dos sensores ou coletores, e se necessário, ajustes na infraestrutura, e os testes da solução, sob supervisão da CONTRATANTE;

4.3.4. Todos os equipamentos necessários à prestação dos serviços, que forem instalados nas dependências da CONTRATANTE, devem ser de responsabilidade da CONTRATADA, novos e de primeiro uso.

4.3.5. Devem englobar a alocação de equipamentos e/ou softwares necessários à consecução das atividades de segurança da informação e ao atendimento das especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia do fabricante, manutenção, atualização dos produtos e monitoramento de segurança em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano.

4.3.6. Os softwares ofertados devem estar licenciados pela CONTRATADA, ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço.

4.3.7. Os equipamentos e softwares não podem constar, no Plano de Implantação, em listas de end-of-lifesale, end-of-support, end-of-life ou similares do fabricante, ou seja, não podem ter previsão de descontinuidade de fornecimento, suporte ou vida;

4.3.8. Toda instalação e configurações deverão ser acompanhadas pela equipe técnica da CONTRATANTE;

4.3.9. A CONTRATADA será responsável por dimensionar a solução a ser adotada na rede da CONTRATANTE. Esta solução estará sujeita à análise e aprovação da equipe técnica da CONTRATANTE;

4.3.10. A solução apresentada não pode causar impacto no funcionamento da rede (por exemplo, lentidão na rede local, degradação no desempenho das estações de trabalho e servidores, entre outros), devendo ser transparente;

4.3.11. Caso o dimensionamento feito pela CONTRATADA para a prestação dos serviços contratados não apresentar desempenho satisfatório, baseado nas recomendações do fabricante e conforme exposto na alínea anterior, a solução deverá ser redimensionada, incluindo adição/substituição de hardware, software, licenças, etc, providos pela CONTRATADA sem ônus adicional para a CONTRATANTE;

4.3.12. Todos os técnicos envolvidos na implantação e configuração devem possuir conhecimentos técnicos aprofundados nos produtos que ficarem sob sua responsabilidade;

4.3.13. Após decretada a conclusão da ativação do serviço pela CONTRATADA, num prazo de 5 (cinco) dias úteis, será iniciada a execução do plano de testes para validação da solução;

4.3.14. A CONTRATADA deverá utilizar a relação das soluções de segurança (ANEXO III) a fim de testar a sua solução proposta antes e depois da implementação da solução;

4.3.15. A CONTRATADA com auxílio da CONTRATANTE irá preparar um Plano de Testes onde devem estar descritos todos os testes a serem realizados a fim de verificar se todas as funcionalidades da solução oferecida e os serviços contratados estão em conformidade ao descrito neste termo de referência;

4.3.16. O Plano de Testes deve ser apresentado em forma de tabela a fim de facilitar o acompanhamento dos mesmos por parte da CONTRATANTE;

4.3.17. Na tabela mencionada na alínea anterior, deve-se incluir os resultados esperados para cada teste realizado;

4.3.18. Os procedimentos descritos no Plano de Testes serão realizados pela CONTRATADA após a implantação e configuração dos produtos. Esses testes serão acompanhados pela equipe técnica da CONTRATANTE e deverá ocorrer em até 10 (dez) dias úteis;

4.3.19. Caso seja detectado qualquer problema nos testes, em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções e, após a realização dessas correções, os testes serão reiniciados;

4.3.20. Se todos os testes forem realizados com sucesso, a solução será considerada implantado, num prazo de 2 (dois) dias úteis, dar-se-á início ao Período de Funcionamento Experimental - PFE, com duração de 10 (dez) dias úteis, para homologação da solução

4.3.21. O PFE - Período de Funcionamento Experimental é estabelecido pela CONTRATANTE para testar o perfeito funcionamento da solução, verificar suas funcionalidades, analisando sua aderência às especificações deste

Edital e seus Anexos, bem como à Proposta da CONTRATADA, e a sua compatibilidade com a estrutura operacional já existente na CONTRATANTE;

4.3.22. Durante o PFE, não deve ocorrer qualquer falha ou interrupção em qualquer uma das funcionalidades da solução fornecida;

4.3.23. A aprovação da solução será vinculada também à entrega da Documentação Técnica – DT e integração com a ferramenta ITSM da CONTRATANTE;

4.3.24. Caso haja qualquer falha ou interrupção em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções e, após a realização destas correções, o PFE será continuado de onde parou.

4.3.25. Caso não haja qualquer falha ou interrupção novamente em qualquer uma das funcionalidades, a solução será considerada homologada.

4.3.26. Para a formalização de que a solução está aprovada e o serviço está em plena operação e disponível, será emitido, em até 10 (dez) dias úteis, Termo de Homologação.

4.3.27. Em até 10 dias úteis após a finalização do PFE, a CONTRATADA apresentará um relatório com a linha base de funcionamento normal, baseado nas recomendações do fabricante, para cada um dos produtos instalados que compõe a solução. Além disso, terão de ser apresentados relatórios periódicos contendo informações de desempenho dos produtos instalados, para que seja identificada com antecedência a necessidade de adição/substituição de hardware/software, conforme descrito no item 4.3.3. Esses relatórios serão apresentados pela CONTRATADA;

4.3.28. Entende-se por relatório de linha base as características de funcionamento padrão dos produtos, identificadas após implementação, realização dos respectivos testes e finalização da PFE;

4.3.29. No Relatório de Linha Base devem ser identificados os aspectos que caracterizam a degradação dos produtos (levando-se em consideração o desempenho, a utilização dos recursos, o throughput, entre outros) e que indicam, consequentemente, a necessidade de upgrade destes.

4.3.30. O serviço contratado deverá estar em plena operação e disponíveis à CONTRATANTE no prazo de, no máximo, 60 (sessenta) dias corridos e contados a partir da emissão da ordem de serviço emitida pela CONTRATANTE;

5. DA ENTREGA

5.1. EQUIPAMENTOS E LICENÇAS DOS ITENS 01, 02, 03, 04, 05, 06, 07 e 08

5.1.1. O prazo de entrega dos equipamentos e as respectivas licenças dos itens é de até 60 (sessenta) dias, contados a partir da assinatura do contrato;

5.1.2. Os equipamentos e licenças 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;

5.1.3. No período de entrega dos equipamentos e licenças a CONTRATADA deve realizar um hands-on composto de parte teórica e prática da solução, capacitando a equipe da CONTRATANTE na realização de tarefas de operação e configuração nos equipamentos, diagnostico de incidentes e monitoramento de indicadores;

5.1.4. O(s) equipamento(s) deve(m) ser novo(s), sem prévia utilização, não remanufaturados, de primeiro uso e acondicionados adequadamente, conforme recomendações do fabricante, de forma a propiciar completa segurança durante o transporte;

5.1.5. Os equipamentos e licenças serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, após a verificação da qualidade, quantidade do material, vigência, e consequente aceitação, mediante termo de recebimento definitivo;

6. LOCAL PARA ENTREGA

6.1. PARA OS ITENS 01, 02, 03, 04 e 05

6.1.1. As entregas deverão ser realizadas pela CONTRATADA na sede da CONTRATANTE situada na Região Metropolitana de Salvador;

6.1.2. As entregas deverão ser realizadas em dias úteis, obedecendo aos horários abaixo discriminados:

6.1.2.1. Segunda a quinta: 08:00hs às 12:00hs e das 13:30hs às 17:30hs;

6.1.2.2. Sexta: 08:00hs às 12:00hs e das 13:30hs às 16:00hs.

6.2. PARA OS ITENS 06, 07 e 08

6.2.1. As entregas deverão ser realizadas pela CONTRATADA na sede da PRODEB, situada na Avenida 4, nº 410, Centro Administrativo da Bahia – CAB, Salvador, Bahia, CEP: 41.745-002;

6.2.2. As entregas deverão ser realizadas em dias úteis, obedecendo aos horários abaixo discriminados:

6.2.2.1. Segunda a quinta: 08:00hs às 12:00hs e das 13:30hs às 17:30hs;

6.2.2.2. Sexta: 08:00hs às 12:00hs e das 13:30hs às 16:00hs.

7. GARANTIA E LICENCIAMENTO DOS ITENS 01 a 08

7.1. No momento da entrega do hardware e software a CONTRATADA deverá apresentar termo de garantia técnica e de licenciamento do software pelo prazo de 24 (vinte e quatro) meses, com cobertura de atendimento on-site, contados a partir da data do recebimento definitivo na CONTRATANTE;

7.2. Ao fim do contrato de garantia e licenciamento, a solução deverá se manter funcional, capaz de criar, customizar e gerenciar políticas e regras, gerar e encaminhar logs, manipular dashboard e entre outras funções necessárias ao manuseio da solução, exceto para funcionalidades que dependam de serviços hospedados em nuvem;

7.3. Para o acompanhamento da garantia, a CONTRATADA deverá disponibilizar profissionais especializados com o objetivo de manter em perfeito estado de operação os serviços e equipamentos;

7.4. Para a garantia técnica, a CONTRATADA deverá observar os procedimentos destinados a recolocar em perfeito estado de operação os serviços e equipamentos tais como:

7.4.1. No que tange ao hardware: desinstalação, reconfiguração ou reinstalação decorrentes de falhas no hardware, fornecimento de peças de reposição, substituição de hardware, atualização da versão de drivers, firmwares e software básico, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

7.4.2. No que tange a software: desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

7.4.3. O provimento de toda e qualquer evolução de software, incluindo correções, "patches", "fixes", "updates", "service packs", novas "releases", "versions", "builds", "upgrades", englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia técnica especificado;

7.4.4. Deve permitir o acesso à base de conhecimento da solução;

7.5. Deve possuir serviço de RMA (Return Merchandise Authorization ou Retorno de Mercadoria Avariada, em português) com envio de equipamentos em até 36 horas úteis e estar licenciado pelo período de 24 (vinte e quatro) meses;

7.6. A manutenção técnica corretiva será realizada sempre que solicitada pelo CONTRATANTE por meio da abertura de chamado técnico diretamente no FABRICANTE ou na CONTRATADA via telefone, Internet ou e-mail;

7.7. No atendimento aos chamados técnicos abertos, deverá ser disponibilizado suporte personalizado por analista(s) designado(s);

7.8. Um chamado técnico somente poderá ser fechado após a confirmação do responsável do CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado;

7.9. A prioridade de atendimento aos chamados será definida pelo CONTRATANTE;

7.10. Na abertura de chamados técnicos, serão fornecidas informações como: número de série e código do equipamento, anormalidade observada, nome do responsável pela solicitação do serviço, versão do software utilizada no hardware e severidade do chamado;

7.11. Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços e ainda:

7.11.1. A CONTRATADA após a realização dos serviços de manutenção deverá apresentar um Relatório contendo identificação do chamado, data e hora de abertura do chamado, data e hora do início e término do atendimento, identificação do defeito, técnico responsável pela solução, as providências adotadas e outras informações pertinentes. Este relatório deverá ser homologado pela CONTRATANTE, através do gestor do contrato;

7.11.2. Os acionamentos dos serviços serão requisitados por meio de chamados (tickets), a serem abertas pelo CONTRATANTE através de número de telefone nacional disponibilizado pela CONTRATADA. Alternativamente os chamados poderão ser abertos por e-mail ou site, desde que a utilização deste canal seja célere o suficiente para permitir o adequado atendimento ao objeto contratual;

7.11.3. Caso seja impossível a substituição dos equipamentos, componentes, materiais ou peças por outras que não as que compõem o item proposto, esta substituição obedecerá ao critério de compatibilidade, que poderá ser encontrado no site do fabricante, através de equivalência e semelhança, e só poderá ser efetuada mediante expressa autorização da PRODEB, para cada caso particular. Caso a PRODEB recuse o equipamento, componente, material e ou peça a ser substituído, o licitante deverá apresentar alternativas, porém o prazo para solução do problema não será alterado;

7.12. Não haverá limitação no número de chamados que poderão ser abertos;

7.13. A CONTRATADA manterá registro de todos os chamados abertos, disponibilizando, para cada um, no mínimo as seguintes informações:

7.13.1. Número sequencial da ordem;

7.13.2. Data e hora de abertura;

7.13.3. Severidade;

7.13.4. Descrição do problema;

7.13.5. Data e hora do início do atendimento;

7.13.6. Data e hora de término do atendimento (solução).

8. CRONOGRAMA

8.1. Para os Itens 01 a 08

ATIVIDADES	PRAZO
Início do planejamento para elaboração do Plano de Instalação, Configuração, migração e demais ações conjunto com a CONTRATANTE dos Itens 01 a 08	Até 10 dias após a assinatura do contrato
Prazo de Entrega dos Equipamentos (Itens 01 a 08) e hands-on do produto.	Até 60 dias a partir da assinatura do contrato
Recebimento Provisório dos Equipamentos e Licenças	Até 05 dias após Entrega dos Equipamentos
Recebimento Definitivo dos Equipamentos testados em funcionamento e licenças ativadas com a validade solicitada no TR	Até 05 (cinco) dias úteis após o recebimento provisório
Início da Instalação da Solução	Até 15 dias após o recebimento definitivo
Conclusão da Instalação da Solução	Até 10 dias após Início da Instalação da Solução
Entrega da Documentação Final	Até 10 dias após Conclusão da Instalação, Configuração
Resolução de Inconformidades	Até 03 dias após validação inicial da CONTRATANTE
Emissão do Termo de Homologação	Até 10 dias após entrega da Documentação Final sem inconformidades

8.2. Para o Item 09

ATIVIDADES	PRAZO
Início do planejamento para elaboração do do Plano de Implantação em conjunto com a CONTRATANTE	Até 5 (cinco) dias após a emissão da Ordem de Serviço
Apresentação dos relatórios da avaliação do ambiente e diagnóstico inicial das vulnerabilidades existentes da CONTRATANTE	Até 30 dias após a emissão da Ordem de Serviço
Implementação do Centro de Operações	Até 60 dias após a emissão da Ordem de Serviço
Conclusão da ativação do Serviço de Monitoramento	Conforme cronograma definido no Plano de Implantação
Início da execução do Plano de Testes para validação da solução	5 dias úteis após a conclusão da ativação do serviço
Execução do Plano de Testes para validação da solução	10 dias úteis após seu início
Início do Período de Funcionamento Experimental – PFE	2 dias úteis após a conclusão do plano de testes
Fim do Período de Funcionamento Experimental – PFE	10 dias úteis após seu início
Entrega da Documentação Final e Relatório de Linha Base	Até 10 dias após Conclusão do Fim do Período de Funcionamento Experimental – PFE
Resolução de Inconformidades	Até 03 dias após acionamento da CONTRATANTE
Emissão do Termo de Homologação	Até 10 dias após entrega da Documentação Final
Emissão da primeira nota fiscal	30 dias após a emissão do Termo de Homologação

8.3. Para os Itens 10 a 13

ATIVIDADES	PRAZO
Início do planejamento para elaboração do do Plano de Implantação em conjunto com a CONTRATANTE	Até 5 (cinco) dias após a emissão da Ordem de Serviço
Conclusão da ativação do Serviço de Monitoramento	Conforme cronograma definido no Plano de Implantação
Entrega da Documentação Final	Até 10 dias após Conclusão da Ativação
Resolução de Inconformidades após Termo de Homologação	Até 03 dias após acionamento da CONTRATANTE
Emissão do Termo de Homologação	Até 10 dias após entrega da Documentação Final
Emissão da primeira nota fiscal	30 dias após a emissão do Termo de Homologação

9. ACORDO DE NÍVEL DE SERVIÇO – ANS DOS ITENS 09 a 13

9.1. Métricas e Convenções

9.1.1. Os Serviços Profissionais de Monitoramento e Segurança deverão ser prestados, no regime (24x7) vinte e quatro horas por dia, sete dias por semana, pelo período da contratação;

9.1.1.1. Plantão Telefônico por número 0800 como serviço de uso ilimitado, no período de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana;

9.1.1.2. Local (on site) exclusivamente nas unidades localizadas da CONTRATANTE localizadas no Estado da Bahia, serviço de uso ilimitado, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tipos de atendimento local: suporte para up-grade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; atualização simultânea nos ambientes dos Órgãos e Entidades da CONTRATANTE.

9.1.2. Não serão consideradas indisponibilidades as seguintes situações:

9.1.2.1. Janela de manutenção previamente acordada entre CONTRATANTE e CONTRATADA;

9.1.2.2. Chamados escalados para o fabricante, em tratamento por este;

9.1.2.3. Indisponibilidade da CONTRATANTE em realizar terefas que dependam desta;

9.1.2.4. 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;

9.1.2.5. Paradas ocasionadas nos equipamentos por erros de configuração causados pelo CONTRATANTE, sem responsabilidade da CONTRATADA;

9.1.2.6. Paradas ocasionadas por casos fortuitos ou de força maior, devidamente comprovados.

9.2. Condições gerais para todos os serviços:

9.2.1. Inicialmente o atendimento poderá ser realizado por meio de atendimento remoto onde ao se identificar a necessidade de atendimento local (on-site), a CONTRATADA deverá deslocar um profissional à unidade, para continuidade do atendimento;

9.2.2. O atendimento no local (on-site) deverá ser provido no ambiente tecnológico da PRODEB e nas Unidades da CONTRATANTE localizadas no Estado da Bahia;

9.2.3. A CONTRATADA deverá responder aos acionamentos, dentro dos prazos fixados neste item, a partir da abertura do acionamento;

9.2.4. O término do atendimento deverá ocorrer dentro dos prazos fixados neste item, a partir do contato da equipe técnica da CONTRATADA, responsável pelo atendimento;

9.2.5. A abertura dos chamados deverá, sempre que possível, ser realizada a partir dos alertas registrados pela solução de monitoramento da CONTRATADA, constanto todos os detalhes para que a equipe de responsta a incidentes realize o atendimento considerando os Níveis de Acordo de Serviço fixados nas tabelas abaixo;

9.2.5.1. A CONTRATADA deverá realizar a integração das soluções de segurança da CONTRATANTE com seu sistema de monitoramento para prover o registro dos chamados automatizados;

9.2.5.2. Em caso de impossibilidade, esta deve ser justificada à CONTRATANTE, onde deverá ser elaborado um procedimento operacional para que os analistas da CONTRATADA possam realizar o registro do chamado de forma imediata na medida que a solução de segurança registre o alerta;

9.2.6. Entende-se por início do atendimento a hora do contato da equipe técnica de suporte da CONTRATADA com a equipe da CONTRATANTE;

9.2.7. Entende-se por término de atendimento a disponibilidade do produto para uso em perfeitas condições de funcionamento no local onde esteja instalado;

9.2.8. O nível de severidade e prioridade deverá ser informado pela CONTRATANTE no momento da abertura de cada chamado. A severidade e prioridade dos chamados será definida considerando critérios de impacto e urgência conforme descrito em cada tabela abaixo;

9.2.9. O nível de severidade e prioridade poderá ser reclassificado a critério da CONTRATANTE. Caso isso ocorra, haverá o início de nova contagem de prazo, conforme o novo nível de severidade.

9.2.10. Todas as solicitações deverão ser registradas pela CONTRATADA, para acompanhamento e controle da execução dos serviços.

9.2.11. A CONTRATADA deverá apresentar relatório de atendimento para cada solicitação de suporte, contendo data e hora da solicitação de suporte técnico, início e término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes.

9.2.12. O relatório de atendimento deverá ser assinado pelo servidor da CONTRATANTE que solicitou o suporte técnico.

9.2.13. Após a conclusão do serviço é obrigação da CONTRATADA verificar o restabelecimento das condições operacionais normais;

9.2.14. Todo o chamado somente será caracterizado como "encerrado" mediante concordância da CONTRATANTE;

9.2.15. Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, este deverá ser programado e planejado, com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da CONTRATANTE.

9.2.16. Para o acompanhamento e avaliação dos serviços da CONTRATADA será estabelecido e utilizado entre as partes os Níveis Mínimos de Serviço. O NMS deve ser considerado e entendido pela CONTRATADA como um compromisso de qualidade que assumirá junto ao CONTRATANTE.

9.2.17. Os NMS para chamados de incidente, requisições e resposta a incidentes deverão ser baseados nos limites estabelecidos nesse item e devem ser configurados e parametrizados no sistema de atendimento de chamados com base no catálogo de serviços a ser acordado entre a CONTRATANTE e a CONTRATADA para um melhor acompanhamento e medição;

9.2.18. A CONTRATADA deverá acompanhar os Indicadores para que seja possível uma avaliação da qualidade do serviço entregue. A partir das informações obtidas nestes indicadores será possível a aplicação do NMS (Níveis Mínimos de Serviço) no processo de pagamento.

9.2.19. A ausência de dados coletados pela CONTRATADA poderá ser considerada indisponibilidade.

9.2.20. Caso ocorra, a qualquer tempo, a não aceitação, por parte do CONTRATANTE, de quaisquer aspectos necessários à declaração da fatura, os prazos para ateste serão descontinuados e reiniciados após a correção necessária. O CONTRATANTE pode, a qualquer momento, recusar-se a declarar a fatura, caso constate:

9.2.21. O valor a ser pago pela realização dos serviços objeto deste contrato será apurado em razão do cumprimento do NMS, podendo diante de eventuais imperfeições em sua execução, resultar em glosa no seu pagamento.

9.2.22. Entretanto, eventuais falhas e descumprimentos contratuais verificados serão devidamente apurados em processos administrativos próprios, podendo resultar em aplicação de penalidade, sem prejuízo de possível rescisão do contrato, na forma prevista na lei.

9.2.23. A CONTRATADA terá até 05 (cinco) dias úteis do mês posterior ao mês faturado para justificar situações imprevistas que tenham gerado uma informação inadequada de faturamento, bem como para comprovar eventuais ocorrências decorrentes de força maior, alheias ao seu controle, que tenham prejudicado o atendimento às condições aqui definidas. Após esse período de justificativa por parte da CONTRATADA, o CONTRATANTE terá até 05 (cinco) dias úteis para análise das justificativas, acatando-as ou não. Após estes 10 (dez) dias úteis, a fatura deve ser recalculada, se for o caso, e encaminhada para o pagamento.

9.3. Níveis Mínimos de Serviço dos Serviços Profissionais de Monitoramento e Segurança

9.3.1. **Níveis Mínimos de Serviço para atendimento a INCIDENTES OPERACIONAIS:**

9.3.1.1. Incidentes operacionais são aqueles que afetam diretamente as soluções de segurança gerenciadas e monitoradas pela CONTRATADA e consequentemente o funcionamento dos serviços do Governo do Estado que dependem delas para o seu pleno funcionamento;

9.3.1.2. O tempo do início efetivo de atendimento ao chamado técnico deverá ser de acordo com a Tabela de Severidade do Incidente, a ser definido pela CONTRATANTE ou proativamente pela equipe de monitoramento da CONTRATADA com base na descrição da tabela, contado a partir da abertura do mesmo não devendo ultrapassar os prazos estabelecidos para as respectivas severidades, contados a partir da abertura do chamado técnico;

9.3.1.3. Tabela de severidades para **INCIDENTES**:

Severidade	Descrição		
1 – Crítica	A solução de segurança não está operante e não é possível nenhuma solução de contorno viável. Problema na solução que gera indisponibilidade em sistemas/serviços produtivos que dependem desse ativo.		
2 – Alta	Problema na solução de segurança que gera impacto em determinado sistema/serviço produtivo que dependem desse ativo.		
3 – Média	Problema contornável que não gera qualquer impacto aos sistemas/serviços produtivos que dependem desses ativos.		
4 – Baixa	Consultas técnicas e dúvidas sobre as soluções de segurança		
Severidade	**Prazo de atendimento**		
	TMIA	**TMSO**	**TMSD**
1 – Crítica	15 min	2h	24h
2 – Alta	30 min	4h	48h
3 – Média	1 h	8h	72 h
4 – Baixa	2h	16h	144h

9.3.1.4. Entende-se por:

9.3.1.4.1. TMIA - Tempo máximo para início de atendimento: Tempo máximo requerido para o início do atendimento;

9.3.1.4.2. TMSO - Tempo máximo para solução operacional: Tempo máximo de recuperação, ou seja, tempo requerido para contornar o problema e deixar a solução/sistema/serviço disponível;

9.3.1.4.3. TMSDC - Tempo máximo para solução definitiva do chamado: Tempo máximo requerido para solucionar em definitivo a causa do problema;

9.3.1.5. Um chamado somente poderá ser fechado após confirmação de responsável do CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento;

9.3.1.6. Este serviço deve estar disponível para acionamento e atendimento no sistema 24x7 (vinte e quatro horas por dia, sete dias na semana);

9.3.2. **Níveis Mínimos de Serviço para REQUISIÇÕES**

9.3.2.1. Requisições são todas as solicitações realizadas pela CONTRATANTE e por seus respectivos usuários e clientes para que a CONTRATADA realize determinada tarefa estabelecida no portfólio de serviços que será elaborado entre as partes;

9.3.2.2. O tempo do início efetivo de atendimento ao chamado técnico deverá ser de acordo com a Tabela de Prioridade da Requisição, a ser definido pela CONTRATANTE ou proativamente pela equipe de monitoramento da CONTRATADA com base na descrição da tabela, contado a partir da abertura do mesmo não devendo ultrapassar os prazos estabelecidos para as respectivas prioridades, contados a partir da abertura do chamado técnico;

9.3.2.3. Tabela de prioridades para **REQUISIÇÕES**:

Prioridade	Descrição
1 – Crítica	Requisições que impactam diretamente na segurança e integridade dos serviços/sistemas considerados críticos no portfolio da CONTRATANTE, ameaçam a continuidade dos serviços ou representam riscos iminentes.

2 – Alta	Requisições que têm um impacto significativo, mas não imediatamente crítico. Podem afetar operações importantes ou serviços que não são considerados como críticos no portfolio da CONTRATANTE.
3 – Média	Requisições que afetam operações ou usuários de forma limitada, sem impacto imediato nos serviços essenciais.
4 – Baixa	Requisições que têm baixo impacto operacional, geralmente tarefas de manutenção preventive, geração de relatórios, consultas ou informações não críticas

Prioridade	**Prazo de atendimento**	
	TMIA	**TMS**
1 – Crítica	15 min	2h
2 – Alta	30 min	4h
3 – Média	1 h	8 h
4 – Baixa	2h	16h

9.3.2.4. Entende-se por:

9.3.2.4.1. TMIA - Tempo máximo para início de atendimento: Tempo máximo requerido para o início do atendimento;

9.3.2.4.2. TMS - Tempo máximo para solução: Tempo máximo requerido para solucionar a requisição;

9.3.2.5. Um chamado somente poderá ser fechado após confirmação de responsável do CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento;

9.3.2.6. Este serviço deve estar disponível para acionamento e atendimento no sistema 24x7 (vinte e quatro horas por dia, sete dias na semana);

9.3.3. **Níveis Mínimos de Serviço para atendimento a RESPOSTA A INCIDENTES DE SEGURANÇA:**

9.3.3.1. Incidentes de segurança referem-se a eventos ou ações que comprometem ou que possam comprometer a integridade, confidencialidade ou disponibilidade de sistemas, redes ou dados da CONTRATANTE. Esses incidentes podem ser causados por ameaças externas, como ataques de hackers, malware, phishing, entre outros, ou por falhas internas de segurança, como erros humanos ou falhas no sistema

9.3.3.2. O tempo do início efetivo de atendimento ao chamado técnico deverá ser de acordo com a Tabela de Severidade do Incidente, a ser definido pela CONTRATANTE ou proativamente pela equipe de monitoramento da CONTRATADA com base na descrição da tabela, contado a partir da abertura do mesmo;

9.3.3.3. Após o início do atendimento, o tempo de solução do operacional e definitiva do incidente deverá ser de acordo com as tabelas abaixo, não devendo ultrapassar os prazos estabelecidos para as respectivas severidades, contados a partir da abertura do chamado técnico;

9.3.3.4. Tabela de severidades para **INCIDENTES DE SEGURANÇA**:

Severidade	**Descrição**
1 – Crítica	Incidentes com níveis de risco crítico ou vulnerabilidades consideradas como críticas, identificadas pelas soluções de segurança, probabilidade de materialização ou com materialização confirmada de risco de impacto crítico que poderia afetar a operação da CONTRATANTE, como um ataque cibernético que cause uma indisponibilidade em qualquer serviço
2 – Alta	Incidentes com níveis de risco alto ou vulnerabilidades consideradas como altas, identificadas pelas soluções de segurança, probabilidade de materialização ou com

	materialização confirmada de risco de impacto alto que poderia afetar a operação da CONTRATANTE, como um ataque cibernético que cause uma degradação em qualquer serviço		
3 – Moderada	Incidentes com possível materialização de risco de impacto moderado ou vulnerabilidades consideradas como médias, como uso inadequado de recursos tecnológicos ou configurações incorretas que precisam ser ajustadas		
4 – Baixa	Este nível de severidade é aplicado para solicitação de configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento dos serviços contratados ou equipamentos fornecidos		
Severidade	**Prazo de atendimento**		
	TMIR	**TMCI**	**TMR**
1 – Crítica	15 min	2h	24h
2 – Alta	30 min	4h	48h
3 – Média	1 h	8h	72 h
4 – Baixa	2h	16h	144h

9.3.3.5. Entende-se por:

9.3.3.5.1. TMIR - Tempo máximo para início de resposta: Tempo máximo requerido para o início da resposta ao incidente de segurança;

9.3.3.5.2. TMCI - Tempo máximo de contenção do incidente: Tempo máximo contenção do incidente de segurança;

9.3.3.5.3. RMR - Tempo máximo de resposta ao incidente: Tempo máximo requerido identificação, contenção e mitigação ou proposição de mitigações do incidente de segurança;

9.3.3.6. Um chamado somente poderá ser fechado após confirmação de responsável do CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento;

9.3.3.7. Este serviço deve estar disponível para acionamento e atendimento no sistema 24x7 (vinte e quatro horas por dia, sete dias na semana);

10. DESCONTOS POR DESCUMPRIMENTO DOS NÍVEIS DE SERVIÇO DOS ITENS 09 a 13

10.1. Na hipótese de não atendimento aos níveis de serviço especificados, sem prejuízo das sanções administrativas previstas nos artigos 211 a 222 do regulamento de licitações e contratos da CONTRATANTE, serão aplicados os descontos:

Penalidades por cada hora completa que exceder os níveis de acordo	Severidade Incidentes Operacionais	Severidade Incidentes de Segurança	Prioridade de Requisições
0,4%	1	1	1
0,3%	2	2	2
0,2%	3	3	3
0,1%	4	4	4

10.2. Os descontos previstos na tabela acima serão calculados tomando como base o valor mensal do contrato e serão descontadas do valor dos pagamentos devidos à CONTRATADA, ou, no caso de inexistência de crédito em seu favor, da garantia contratual prestada pela empresa contratada;
10.3. O valor do desconto no período será igual ao somatório das ocorrências de não atendimento ou solução nos níveis de serviço especificados;
10.4. Os descontos aplicados só poderão ser relevados motivadamente e por conveniência administrativa, mediante ato da autoridade competente, devidamente justificado;
10.5. 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;
10.6. A garantia deverá ser restabelecida integralmente, caso tenha incidido qualquer desconto sobre o valor desta;
10.7. O período inicial de 90 (noventa) dias após a emissão de Termo de Homologação confirmando o término da implantação e homologação dos serviços, será considerado como período de estabilização da operação dos serviços, durante o qual, os indicadores de serviço não atingidos, terão aplicadas as glosas conforme disposto no Tópico Acordo de Níveis de Serviço, de acordo com os seguintes critérios:
10.7.1. Nos primeiros 30 (trinta) dias: aplicar-se-á, efetivamente, 25% (vinte e cinco por cento) dos percentuais previstos na tabela para cada ocorrência de indicadores de serviço não atingido;
10.7.2. Do 31º ao 60º dia: aplicar-se-á, efetivamente, 50% (cinquenta por cento) dos percentuais previstos na tabela para cada ocorrência de indicadores de serviço não atingido;
10.7.3. Do 61º ao 90º dia: aplicar-se-á, efetivamente, 75% (setenta e cinco por cento) dos percentuais previstos na tabela para cada ocorrência de indicadores de serviço não atingido
10.7.4. Após o 90º dia, aplicar-se-ão integralmente os percentuais previstos na tabela para cada ocorrência de indicadores de serviço não atingido
10.8. Caso haja prorrogação de vigência contratual, não haverá novo período de estabilização;

V. 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 por parte da PRODEB.
11.2. A existência de preços registrados não obriga firmar contratações que deles poderão advir, ficando-lhe facultada 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 PRODEB faculta aos Órgãos e Entidades da Administração Pública do Estado da Bahia a adesão à ata de Registro de Preços por ela firmada, disponibilizando no instrumento convocatório da licitação como anexos, minutas de contratos destinados ao atendimento das demandas da Companhia, bem como para atendimento dos órgãos não participantes, conforme previsto no Art.157, §7º do RLC da Prodeb.
11.4. Com base no Decreto Estadual 19.252/2019, as aquisições ou contratações adicionais a que se refere este item não poderão exceder, por órgão ou entidade, a 50% dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes. As adesões à ata de registro de preços são limitadas, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que eventualmente aderirem.
11.5. Órgãos e Entidades da Administração Pública do Estado da Bahia, assim como as Empresas Públicas e Sociedades de Economia Mista que não participaram do registro de preços, quando desejarem fazer uso da ata de registro de preços, deverão consultar a PRODEB.
11.6. 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, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com a PRODEB.
11.7. Compete ao órgão não participante os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências à PRODEB.
11.8. A ata de registro de preço se destinará ao atendimento das demandas, compreendendo o território do Estado da Bahia;
11.9. O prazo de validade da ata de registro de preços será de 12 (doze) meses, a contar da data de sua assinatura.

12. CRITÉRIOS DE ACEITABILIDADE DA PROPOSTA

12.1. Não serão admitidas as propostas que desobedeçam aos critérios dispostos 42, IX do Regulamento de Licitações e Contratos da PRODEB;

12.2. A Proponente deverá referenciar explicitamente em sua proposta, a origem de fabricação do(s) equipamento(s) ofertado(s), bem como nome(s) do(s) fabricante(s), códigos e part numbers de todas as partes que compõem os equipamentos sendo propostos de forma a deixar claro o atendimento de acordo com o exigido no edital;

12.3. A Proponente deverá apresentar manuais, documentos ou datasheets oficiais do fabricante em língua portuguesa ou inglesa. Para cada item desta especificação deverá ser referenciado a página e o capítulo que comprova o seu atendimento (planilha ponto a ponto);

12.4. A Proponente deverá apresentar todas as soluções, necessárias ao cumprimento dos requisitos de serviço elencados neste Termo de Referência, e que não façam parte das soluções instaladas na PRODEB e que serão fornecidas, sem ônus adicional para a CONTRATANTE, em quantidade suficiente para o escopo do ambiente de DataCenter;

12.5. 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;

12.6. Deverão estar inclusas no valor dos serviços, 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;

12.7. As propostas precisam conter a razão social do fornecedor, telefone para contato, preposto responsável, CNPJ, além de estarem devidamente assinadas e datadas;

12.8. A proposta deverá ter o seu prazo de validade não inferior a 60 (sessenta) dias da sua emissão;

12.9. Deverá ser apresentada juntamente com a proposta, uma declaração 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;

12.9.1. A exigência contida no item acima tem o objetivo de resguardar os interesses da CONTRATANTE, comprovando a aptidão da contratada para realizar o serviço de suporte, bem como, garantindo o acesso a atualizações corretivas e evolutivas disponibilizadas pelo fabricante durante o curso do prazo de vigência do contrato;

12.10. A proposta deverá descrever os preços de forma clara e precisa, os modelos dos equipamentos propostos para atendimento às especificações técnicas constantes deste Termo de Referência;

12.11. A proposta deve ser apresentada contendo as Especificações Técnicas a seguir:

12.11.1. Informações sobre hardware e software, constando marca e modelo, fabricante e velocidades das portas;

12.11.2. Manuais ou datasheets oficiais do(s) fabricante(s);

12.11.3. Planilha indicando a localização nos manuais, páginas web e/ou datasheets referenciado, comprovando o atendimento a cada item da especificação exigida neste Termo de Referência (planilha ponto a ponto);

12.12. A não comprovação de qualquer dos itens acima implicará na imediata desclassificação da proponente.

13. CONDIÇÕES PARA ASSINATURA DO CONTRATO

13.1. Como condição para assinatura do contrato, a empresa deverá apresentar:

13.1.1. Comprovação de no mínimo, 08 (oito) profissionais técnicos qualificados, devidamente treinados pelo fabricante para instalar, configurar e manter a solução de Segurança do Fabricante, devendo estes treinamentos técnicos serem comprovados por certificados de qualificação técnica vigentes;

14. MODALIDADE DE LICITAÇÃO

14.1. O procedimento indicado para a licitação é o rito similar ao da modalidade pregão e o critério de julgamento a ser adotado é o menor preço global, conforme exposto nos artigos 52, IV, e 55, I, ambos do Regulamento de Licitações e Contratos da PRODEB, respeitando o valor unitário referencial de cada item do lote único;

14.2. A licitação deverá ser processada eletronicamente, em razão do quanto estabelecido no art. 4º, VI, do RLC da PRODEB;

14.3. A licitação será processada em lote único, visto que para formação de preços dos Serviços Profissionais de Monitoramento e Segurança a licitante precisará tanto das informações das soluções de segurança que estão instaladas na PRODEB, relacionadas no ANEXO III, e das soluções de segurança dos itens 1 a 13 que são ofertadas pela mesma. Além disso, com as soluções ofertadas pela licitante, haverá um melhor gerenciamento, monitoramento e operação, além de estarem intrinsecamente relacionados;

14.4. O certame adotará o modo de disputa aberto;

14.5. No intuito de evitar o oferecimento de lances com variação insignificante, os lances ofertados deverão observar um intervalo mínimo de diferença de valores, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta, que deverá ser R$ 1.000,00 (um mil reais);

15. QUALIFICAÇÃO TÉCNICA

15.1. A PROPONENTE deve apresentar o atestado de capacidade técnica emitido por empresa pública ou privada comprovando que forneceu soluções de Next-Generation Firewalls (NGFW), soluções para Endpoints, Email, Autenticação de Múltiplos Fatores (MFA) e prestou serviços de implantação, suporte, garantia e serviços gerenciados de segurança da informação englobando operação, atendimento de requisições, monitoramento, gestão de incidentes e vulnerabilidades, com características semelhantes às especificadas neste Termo de Referência;

15.1.1. Os atestados deverão ser impressos em papel timbrado, com nome e telefone de contato dos responsáveis pela informação atestada, não sendo aceitas declarações genéricas de catálogos, manuais de Internet, devendo ainda atestar a satisfação com o serviço ofertado pela PROPONENTE.

15.2. 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.

16. CONSÓRCIO

16.1. 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:

16.1.1. As empresas consorciadas deverão apresentar, juntamente com os documentos de habilitação jurídica, o Instrumento de Constituição ou a comprovação do 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. 102, II do RLC da PRODEB);

e) outorga à empresa líder de poderes expressos, irretratáveis e irrevogáveis, para representar o consórcio perante o órgão licitante 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. 102, 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. 102, § 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 contratante, até o cumprimento do objeto da licitação com a aceitação definitiva do objeto licitado (art. 102, § 4o, do RLC da PRODEB).

16.2. A empresa líder será responsável pela apresentação do credenciamento.

16.3. No consórcio entre empresas brasileiras e estrangeiras, a liderança caberá, obrigatoriamente, à empresa brasileira, observado o disposto na alínea "d" do item 1.1 (art. 102, § 1o, do RLC da PRODEB).

16.4. Cada uma das empresas consorciadas deverá apresentar, de forma individualizada, mas no mesmo envelope de habilitação, a documentação exigida neste instrumento convocatório para a habilitação (art. 102, inciso III, do RLC da PRODEB).

16.5. 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 (art. 102, inciso III, do RLC da PRODEB).

16.6. 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. 102, inciso V, do RLC da PRODEB).

16.7. 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 (art. 102, §2o, do RLC da PRODEB), ficando esclarecido que o não cumprimento dessa obrigação acarretará as consequências previstas no art. 211 do RLC da PRODEB, uma vez que constitui ilícito administrativo, conforme previsto no art. 212 do RLC, o qual remete ao art. 185, IV da Lei Estadual nº 9.433/2005).

16.8. 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. 102, §4º do RLC da PRODEB).

16.9. 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. 102, §3º do RLC da PRODEB)

17. SUBCONTRATAÇÃO

17.1. É vedada a subcontratação total ou parcial do objeto.

VI. DO PAGAMENTO

18. CONDIÇÕES DE PAGAMENTO

18.1. **PRODEB**

18.1.1. O pagamento referente aos itens 01 ao 08 descritos neste TR, serão realizados em 01 (uma) parcela após a emissão do Termo de Homologação que caracteriza a entrega e instalação das soluções;

18.1.2. O pagamento referente as prestações de serviços previstas nos itens 09 ao 13 descritos neste TR, serão realizados de mensalmente, pelo período em 24 (vinte e quatro) meses em até 30 dias após a emissão do Termo de Homologação, que caracteriza a finalização da implantação e operação dos serviços;

18.1.3. O pagamento ocorrerá de acordo com os prazos estabelecidos no art. 10, do Regulamento de Licitações e Contratos da PRODEB, de acordo com o valor dos bens adquiridos, a saber:

18.1.3.1. até R$ 50.000,00 o pagamento será efetuado em até 15 (quinze) dias;

18.1.3.2. de R$ 50.000,01 a R$ 100.000,00 o pagamento será efetuado em até 30 (trinta) dias;

18.1.3.3. acima de R$ 100.000,01 o pagamento será efetuado em até 45 (quarenta e cinco) dias;

18.1.4. O pagamento somente será autorizado depois de efetuado o "atesto" pela comissão ou servidor competente da CONTRATANTE na nota fiscal apresentada;

18.1.5. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à aquisição, serviço, 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;

18.1.6. A proposta de preços e a nota fiscal de faturamento deverão refletir o objeto da aquisição, sendo necessário o detalhamento da composição do objeto/item. Esse deverá ser detalhado na proposta apresentada pela LICITANTE e reproduzido integralmente na respectiva nota fiscal de faturamento;

18.1.7. A CONTRATADA deverá enviar as notas fiscais e documentos relacionados ao pagamento para o e-mail: cofic.financeiro@prodeb.ba.gov.br;

18.1.8. Antes da realização do pagamento deverá ser comprovada pela CONTRATADA a manutenção das condições de habilitação exigidas no edital.

18.2. ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA DO ESTADO DA BAHIA:

18.2.1. O pagamento referente aos itens 01 ao 08 descritos neste TR, serão realizados em 01 (uma) parcela após a emissão do Termo de Homologação que caracteriza a entrega e instalação das soluções;

18.2.2. O pagamento referente as prestações de serviços previstas nos itens 09 ao 13 descritos neste TR, serão realizados mensalmente, pelo período em 24 (vinte e quatro) meses, em até 30 dias após a emissão do Termo de Homologação, que caracteriza a finalização da implantação e operação dos serviços;

18.2.3. Os pagamentos devidos à CONTRATADA serão efetuados através de ordem bancária ou crédito em conta corrente, no prazo não superior a 08 (oito) dias úteis, contados da data da apresentação da fatura, em consonância com o disposto no art. 6°, §5°; art. 8°, XXXIV; art. 79, XI, "a"; art. 154, V e art. 155, V da Lei estadual no 9.433/05.

19. JUSTIFICATIVA DE PREÇO

19.1. Devido a tratar-se de registro de preços com a previsão de saque da ata pela PRODEB (Sociedade de Economia Mista), Órgãos e Entidades da Administração Pública do Poder Executivo Estadual, é necessário respeitar as respectivas legislações. Deste modo, nos termos do art. 81, da Lei Estadual nº 9.433/2005, constitui o anexo do edital, dele fazendo parte integrante, o orçamento estimado e planilhas de quantitativos e preços unitários. Portanto, é necessário tornar público o valor referencial do objeto da licitação, em atendimento a citada Lei de Licitações e conforme facultado de forma excepcional no art. 43, do RLC da PRODEB.
19.2. O valor referencial foi obtido seguindo o rito do Art. 47 do RLC da PRODEB, sendo apurado a partir do menor valor entre as propostas recebidas.
19.3. Orçamento estimado e planilhas de quantitativos e preços unitários conforme ANEXO IV.

VII. DO CONTRATO

20. VIGÊNCIA DO CONTRATO

20.1. O Contrato terá prazo de vigência de 28 (vinte e oito) meses, a partir da data de assinatura, podendo ser prorrogado para os itens 1 e 2 e os serviços dos itens 09 a 13 até o limite de 60 (sessenta) meses, conforme previsto no art. 164, do Regulamento de Licitações e Contratos da PRODEB.

21. CONSIDERAÇÕES GERAIS

21.1. A execução dos serviços objeto deste Termo de Referência, incluindo suas implementações, deverá, obrigatoriamente, ser efetuada de forma a não afetar o funcionamento dos serviços já em operação;
21.2. No caso de necessidade de interrupção de outros serviços ou equipamentos, em decorrência da instalação a ser efetuada, esta deverá ser devidamente planejada e acordada com a PRODEB;
21.3. Os serviços, objeto desta licitação, deverão ser executados sob a inteira responsabilidade funcional e operacional da CONTRATADA, sobre cujos empregados deverá manter estrita e exclusiva fiscalização;
21.4. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e os CONTRATANTES, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta;
21.5. Toda a equipe de profissionais da CONTRATADA deverá portar identificação quando da execução dos serviços;
21.6. Toda a equipe de profissionais da CONTRATADA deverá usar equipamento de segurança conforme cada atividade a ser efetuada;
21.7. As discrepâncias, dúvidas, omissões ou erros observados devem ser levados ao conhecimento do CONTRATANTE, de modo a serem esclarecidas todas as possíveis dúvidas, antes do início da execução, evitando-se, assim, embaraços para o perfeito andamento dos serviços.

22. OBRIGAÇÕES CONTRATUAIS

22.1. OBRIGAÇÕES DA CONTRATADA

22.1.1. Zelar pelo cumprimento do objeto e das demais cláusulas deste Termo de Referência e Contrato;
22.1.2. Fornecer os equipamentos e 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;
22.1.3. Os equipamentos(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;
22.1.4. Prestar os serviços de garantia e suporte no sistema 24x7 (vinte e quatro horas por dia, sete dias na semana);
22.1.5. Utilizar cópias legais de software, sistemas operacionais e outros necessários para a realização de suas instalações;
22.1.6. Atender às solicitações de serviços de acordo com as especificações técnicas, cronogramas e condições especificadas;

22.1.7. Prestar os serviços com pessoal adequadamente capacitado em locais e instalações de acordo com as orientações constantes neste Termo de Referência;

22.1.8. 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;

22.1.9. Não veicular publicidade ou qualquer outra informação acerca das atividades objeto deste contrato, sem prévia autorização da CONTRATANTE;

22.1.10. Manter, durante a vigência do contrato, todas as condições de habilitação e qualificação exigidas neste Termo de Referência;

22.1.11. 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;

22.1.12. 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;

22.1.13. Promover a transferência do conhecimento vide (hands-on) de cada produto entregue, para os profissionais da CONTRATANTE, sem ônus adicional;

22.1.14. Realizar a entrega dos hardwares e softwares no tempo estabelecido no edital e 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;

22.1.15. Dar ciência a CONTRATANTE, imediatamente e por escrito, de qualquer anormalidade identificada na execução dos serviços;

22.1.16. 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, 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 PRODEB ou a terceiros;

22.1.17. 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, o que não exclui nem diminui a responsabilidade pelos danos que se constatarem, independentemente do controle e fiscalização exercidos pela CONTRATANTE;

22.1.18. Reparar, exclusivamente às suas custas, todos os defeitos, erros, falhas, omissões e quaisquer irregularidades verificadas nos hardwares, softwares fornecidos e nos serviços, bem como responsabilizar-se por qualquer dano ou prejuízo daí decorrente;

22.1.19. Garantir o atendimento dos prazos definidos neste Termo de Referência, bem como cumprir os prazos do(s) cronograma(s) pactuados de acordo com as especificações contidas neste Termo de Referência, sempre que houver a necessidade de execução de correções em hardwares, software e serviços já entregues.

22.2. **OBRIGAÇÕES DA CONTRATANTE**

22.2.1. **PRODEB**

22.2.1.1. Operar e administrar as soluções adquiridas;

22.2.1.2. Fiscalizar o cumprimento do objeto e das demais cláusulas deste Termo de Referência e seus anexos;

22.2.1.3. Proporcionar as condições necessárias para que a CONTRATADA possa cumprir o que estabelece este Termo de Referência e seus anexos;

22.2.1.4. Receber o objeto no prazo e condições estabelecidas no presente Termo de Referência;

22.2.1.5. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Termo de Referência e da proposta, para fins de aceitação e recebimento definitivo;

22.2.1.6. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

22.2.1.7. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de comissão/servidor especialmente designado;

22.2.1.8. Proporcionar as condições necessárias para que a CONTRATADA possa cumprir o que estabelece este Termo de Referência e seus anexos;

22.2.1.9. Designar pessoas para os papéis descritos quanto à fiscalização;

22.2.1.10. Convocar, realizar e registrar reuniões junto à CONTRATADA;

22.2.1.11. Atestar e homologar a entrega dos hardwares e softwares entregues;

22.2.1.12. Validar a execução dos serviços a serem prestados;

22.2.1.13. Notificar formalmente a CONTRATADA quanto a defeitos ou irregularidades observadas nos hardwares, softwares e na execução dos serviços e sobre a aplicação de penalidades, assegurada sua prévia defesa;

22.2.1.14. Permitir a entrada dos funcionários da CONTRATADA, desde que devidamente identificados, garantindo que tenham acesso aos equipamentos, bem como fornecer todos os meios necessários à execução dos serviços;

22.2.1.15. Efetuar os pagamentos devidos à CONTRATADA no prazo e nas condições indicadas neste instrumento, desde que atenda as formalidades necessárias, e após aceitação dos hardwares, softwares e serviços pelos meios convencionados;

22.2.1.16. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos profissionais da CONTRATADA ou o seu Preposto;

22.2.1.17. Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da CONTRATADA, conforme determina a Lei, antes de efetuar o pagamento devido.

22.2.2. **ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA DO ESTADO DA BAHIA:**

22.2.2.1. O Edital disponibilizará, sob a forma de anexos, as minutas de contratos destinadas ao atendimento das demandas desta Companhia, sob regência da Lei 13.303/2016, assim como aquela aderente aos órgãos que integram à Administração Pubública Direta do Estado da Bahia, autarquias e fundações, regidos pela Lei 9.433/2005.

23. OBRIGAÇÕES DO GESTOR TÉCNICO DA SOLUÇÃO – PRODEB

23.1. Exercer a gestão técnica dos serviços de profissionais e de monitoramento, conforme objeto deste Edital;

23.2. Exercer o planejamento e análise da arquitetura das soluções de segurança necessárias;

24. PROTEÇÃO DE DADOS PESSOAIS

24.1. 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;

24.2. 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;

24.3. 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;

24.4. 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;

24.5. 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;

24.6. 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;

24.7. 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;

24.8. 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;

24.9. 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;

24.10. 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;

24.11. 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;

24.12. 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;

24.13. 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;

24.14. 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;

24.15. 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.

25. ELEMENTOS NECESSÁRIOS À GESTÃO DO CONTRATO

25.1. Para a gestão e fiscalização do contrato será adotado o rito previsto no Capítulo V, Seção III, do Regulamento de Licitações e Contratos da PRODEB. O Gestor e Fiscal do contrato decorrente deste processo serão indicados no momento da contratação.

VIII. INFORMAÇÕES ADICIONAIS

26. FORMA DE COMUNICAÇÃO

26.1. A tramitação de documentos entre CONTRATANTE e a CONTRATADA deverá ser rigorosamente controlada através de documentos protocolados fisicamente ou enviados através de meio eletrônico.

27. SANÇÕES ADMINISTRATIVAS

27.1. Serão aplicadas sanções administrativas ao Licitante que cometer qualquer prática considerada ilícita conforme exposto no Art. 211 a 222 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.

28. TERMO DE COMPROMISSO E DE CONFIDENCIALIDADE

28.1. A CONTRATADA compromete-se a cumprir e obedecer à Política de Segurança da Informação do Governo do Estado da Bahia;

28.2. A CONTRATADA deverá assinar Termo de Compromisso, Sigilo e Confidencialidade, Anexo I deste Termo no momento da assinatura do contrato.

29. GARANTIA CONTRATUAL

29.1. A empresa vencedora do certame deverá prestar garantia contratual de 5% (cinco por cento) do valor do contrato, podendo optar por uma das modalidades previstas no art. 162 do Regulamento de Licitações e Contratos da PRODEB, ficando esclarecido que a garantia contratual deverá ter seu valor atualizado nas mesmas condições do contrato e renovada, quando for o caso, conforme previsto neste Termo de Referência.

30. MATRIZ DE RISCO

30.1. Este Termo de Referência foi elaborado com base nos dados levantados e explicitados no documento denominado MAPA DE RISCOS.

Salvador, 03 de abril de 2024.

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, Salvador-Bahia, 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 mesmasob 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 2023.

_____ _____

Responsável pelo Contrato – CONTRATANTE Responsável pelo Contrato - CONTRATADA

ANEXO II
MODELO DE PROPOSTA

ITENS DE SOFTWARE E HARDWARE					
ITEM	**DESCRITIVO**	**UNID**	**QTD**	**VALOR UNITARIO**	**VALOR TOTAL**
01	Solução de Segurança de Endpoint - EPP	UN	2500		
02	Solução para duplo Fator de Autenticação - Token Mobile	UN	750		
03	Solução de Segurança de Rede NGFW TIPO I	UN	450		
04	Solução de Segurança de Rede NGFW TIPO II	UN	60		
05	Solução de Segurança de Aplicações WAF TIPO I	UN	08		
06	Solução de Segurança de Aplicações WAF TIPO II	UN	02		
07	Solução de Segurança Decoy/Honeypot	UN	04		
08	Solução de Segurança de Email.	UN	02		
VALOR TOTAL AQUISIÇÃO (A)				R$	

ITENS DE SERVIÇO					
ITEM	**DESCRITIVO**	**UNID**	**QTD**	**VALOR UNITARIO MENSAL**	**VALOR TOTAL MENSAL**
09	Serviços Profissionais de Monitoramento e Segurança do Datacenter da PRODEB pelo período de 24 Meses.	UN	1		
10	Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Endpoint - EPP" para cada item monitorado pelo período de 24 Meses.	UN	62.500		
11	Serviços Profissionais de Monitoramento e Segurança para o item "Solução para duplo Fator de Autenticação - Token Mobile" para cada item monitorado pelo período de 24 Meses.	UN	3.750		
12	Serviços Profissionais de Monitoramento e Segurança para os itens "Solução de Segurança de Rede NGFW TIPO I, II" para cada item monitorado pelo período de 24 Meses.	UN	510		
13	Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Aplicações WAF TIPO I" para cada item monitorado pelo período de 24 Meses.	UN	08		
VALOR TOTAL MENSAL SERVIÇOS (B) PAGAMENTO MENSAL				R$	
VALOR TOTAL PARA 24 MESES (C) VALOR TOTAL MENSAL SERVIÇOS (B) X 24 (vinte e quatro) MESES				R$	

VALOR GLOBAL DO LOTE VALOR TOTAL AQUISIÇÃO (A) + VALOR TOTAL PARA 24 MESES (C)	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

<table>
<tr><td rowspan="4">CARIMBO DO FORNECEDOR
(COM CNPJ)</td><td colspan="2">RAZÃO SOCIAL</td></tr>
<tr><td>TELEFONE</td><td>PRAZO DE ENTREGA</td></tr>
<tr><td>DATA</td><td>VALIDADE DA PROPOSTA</td></tr>
<tr><td>CONTATO</td><td>E-MAIL</td></tr>
</table>

ANEXO III
SOLUÇÕES DE SEGURANÇA INSTALADAS NA PRODEB

Produto	Descrição	PartNumber	Qtd.
FortiAnalyzer 3700F	Solução de Logs e Relatoria	FAZ-3700F	2
FortiAnalyzer 2000E	Solução de Logs e Relatoria	FAZ-2000E	2
FortiAuthenticator 3000E	Solução de Autenticação Centralizada	FAC-3000E	2
FortiManager 3000G	Solução de Gerência Centralizada	FMG-3000G	1
FortiManager 3900E	Solução de Gerência Centralizada	FMG-3000G	1
FortiSIEM	Solução de Correlação de eventos, Resposta Automática e Remediação de Incidentes	FSM-AIO-BASE	1
FortiWeb-2000F	Solução de Firewall de aplicações WEB	FWB-2000F	1
FortiADC 400F	Solução de Balanceamento de Carga de Aplicações	FAD-400F	2
FortiGate-3301E	Solução de Next Generation Firewall - NGFW	FG-3301E	2
Solução Trend Micro™ Deep Discovery™ Inspector	Solução de Network Detection and Response	DDI9000	2
NS9500 Sensor	Solução de Intrusion Prevention System	NS9500	2
Trend Workload Security	Agente XDR de segurança de servidores		2250
Trend Endpoint Sensor	Agente XDR de segurança para desktops		500
Fortigate 600D	Solução de Next Generation Firewall – NGFW	FG-600D	2
Fortigate 600F	Solução de Next Generation Firewall – NGFW	FG-600F	2
Fortigate 3000D	Solução de Next Generation Firewall – NGFW	FG-3000D	2
Fortigate 3700F	Solução de Next Generation Firewall – NGFW	FG-3700F	2
Tenable.SC	Solução de Análise e Vulnerabilidade de Infraestrutura		1
Tenable.io	Solução de Análise e Vulnerabilidade de Aplicações		1
Webgateway	Solução de Proxy e módulos	WG-5500D	6
ePO Trellix	Solução de Gerenciamento de EDR e módulos		
EDR Trellix	Solução de EDR e módulos		
Forescout	Solução de Visibilidade, Automação e Controle de Acesso		1

ANEXO IV
TABELA DE VALORES REFERENCIAIS

ITEM	DESCRITIVO	UNID	QUANTIDADE	VALOR REFERENCIAL - MENOR PREÇO	
				Valor Unitário/Mensal	Valor Total/24 meses
1	Solução de Segurança de Endpoint – EPP. Cod. SIMPAS (705109000 07796-8)	UN	2500	R$ 10.820,00	R$ 27.050.000,00
2	Solução para duplo Fator de Autenticação - Token Mobile. Cod SIMPAS (705109000 07800-0)	UN	750	R$ 2.945,00	R$ 2.208.750,00
3	Solução de Segurança de Rede NGFW TIPO I Cod. SIMPAS (705109000 07797-6)	UN	450	R$ 16.094,00	R$ 7.242.300,00
4	Solução de Segurança de Rede NGFW TIPO II. Cod. SIMPAS (705109000 07798-4)	UN	60	R$ 172.400,00	R$ 10.344.000,00
5	Solução de Segurança de Aplicações WAF TIPO I. Cod. SIMPAS (705109000 07793-3)	UN	8	R$ 509.625,00	R$ 4.077.000,00
6	Solução de Segurança de Aplicações WAF TIPO II. Cod. SIMPAS (705109000 07794-1)	UN	2	R$ 1.622.250,00	R$ 3.244.500,00
7	Solução de Segurança Decoy/Honeypot. Cod SIMPAS (705109000 07799-2)	UN	4	R$ 300.510,00	R$ 1.202.040,00
8	Solução de Segurança de Email. – Cod. SIMPAS (705109000 07795-0)	UN	2	R$ 1.213.450,00	R$ 2.426.900,00
9	Serviços Profissionais de Monitoramento e Segurança do Datacenter da PRODEB pelo período de 24 Meses. – Cod. SIMPAS (022409000 07805-0)	UN	1	R$ 446.887,00	R$ 10.725.288,00
10	Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Endpoint - EPP" para cada item monitorado pelo período de 24 Meses. Cod SIMPAS (022409000 07804-2)	UN	62.500	R$ 5,38	R$ 8.070.000,00
11	Serviços Profissionais de Monitoramento e Segurança para o item "Solução para duplo Fator de Autenticação - Token Mobile" para cada item monitorado pelo período de 24 Meses. Cod SIMPAS (022409000 07803-4)	UN	3.750	R$ 7,47	R$ 672.300,00
12	Serviços Profissionais de Monitoramento e Segurança para os itens "Solução de Segurança de Rede NGFW TIPO I, II" para cada item monitorado pelo período de 24 Meses. Cod SIMPAS (022409000 07802-6)	UN	510	R$ 692,35	R$ 8.474.364,00
13	Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Aplicações WAF TIPO I" para cada item monitorado pelo período de 24 Meses. Cod. SIMPAS (022409000 07801-8)	UN	8	R$ 7.980,00	R$ 1.532.160,00
VALOR TOTAL					**R$ 87.269.602,00**

ANEXO V
PLANILHA DE QUANTITATIVOS DOS ÓRGÃOS E ENTIDADES PARTICIPANTES

SIGLA	ÓRGÃO/ENTIDADE	ITEM 01	ITEM 02	ITEM 03	ITEM 04	ITEM 05	ITEM 10	ITEM 11	ITEM 12	ITEM 13
ADAB	Agência de Defesa Agropecuária da Bahia	79	2	0	0	0	1975	10	0	0
AGERBA	Agência Estadual de Regulação Serviços Públicos de Energia Transporte	16	4	2	0	0	400	20	2	0
AGERSA	Agência Reguladora de Saneamento Básico do Estado da Bahia	6	8	0	2	0	150	40	2	0
CASA CIVIL	Casa Civil do Governo do Estado da Bahia	19	10	2	2	2	475	50	4	2
CASA MILITAR	Casa Militar do Governador da Bahia	8	2	0	0	0	200	10	0	0
CBM	Corpo de Bombeiros Militar da Bahia	2	0	0	0	0	50	0	0	0
DPT	Departamento de Polícia Técnica da Bahia	53	0	2	2	0	1325	0	4	0
FAPESB	Fundação de Amparo à Pesquisa do Estado da Bahia	6	25	0	1	0	150	125	1	0
FPC	Fundação Pedro Calmon / SECULT	16	0	0	2	0	400	0	2	0
GABGOV	Gabinete do Governador do Estado da Bahia	16	7	2	2	0	400	35	4	0
IPAC	Instituto do Patrimônio Artístico e Cultural do Estado da Bahia / SECULT	9	0	0	0	0	225	0	0	0
IRDEB	Instituto de Radiodifusão Educativa da Bahia / SECULT	1	0	2	0	0	25	0	2	0
PGE	Procuradoria Geral do Estado da Bahia	1	1	2	2	2	25	5	4	2
PLANSERV	Sistema de Assistência à Saúde dos Servidores Públicos Estaduais	14	0	2	0	0	350	0	2	0
PMBA	Polícia Militar da Bahia	158	40	85	2	0	3950	200	87	0
SAEB	Secretaria da Administração do Estado da Bahia	106	60	2	4	0	2650	300	6	0
SDE	Secretaria de Desenvolvimento Econômico do Estado da Bahia	1	0	0	1	0	25	0	1	0
SDR	Secretaria de Desenvolvimento Rural do Estado da Bahia	1	0	0	1	0	25	0	1	0
SEAGRI	Secretaria da Agricultura, Irrigação e Reforma Agrária	11	40	1	2	0	275	200	3	0
SEAP	Secretaria de Administração Penitenciária e Ressocialização do Estado da Bahia	1	0	20	4	0	25	0	24	0
SEC	Secretaria da Educação do Estado da Bahia	1470	440	271	18	2	36750	2200	289	2
SECTI	Secretaria de Ciência, Tecnologia e Inovação do Estado da Bahia	1	0	0	2	0	25	0	2	0
SEDUR	Secretaria de Desenvolvimento Urbano da Bahia	16	0	0	1	0	400	0	1	0

SEI	Superintendência de Estudos Econômicos e Socias da Bahia	25	3	2	2	0	625	15	4	0
SERIN	Secretária de Relações Institucionais do Estado da Bahia	13	0	0	1	0	325	0	1	0
SESAB	Secretaria de Saúde do Estado da Bahia	344	100	33	4	0	8600	500	37	0
SETRE	Secretaria do Trabalho, Emprego, Renda e Esporte do Estado da Bahia	59	0	20	0	0	1475	0	20	0
SETUR	Secretaria Estadual de Turismo da Bahia	11	0	0	0	0	275	0	0	0
SJDH	Secretaria de Justiça e Direitos Humanos	24	0	1	0	0	600	0	1	0
SSP	Secretaria de Segurança Pública	4	4	0	1	2	100	20	1	2
SUFOTUR	Superintendência de Fomento ao Turismo da Bahia	6	2	0	2	0	150	10	2	0
VICEGOV	Gabinete do Vice-Governador	3	2	1	2	0	75	10	3	0
TOTAL		**2500**	**750**	**450**	**60**	**8**	**62500**	**3750**	**510**	**8**

PRODEB
TECNOLOGIA, INFORMAÇÃO E SEGURANÇA

COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DA BAHIA

*ESTA PLANILHA DEVERÁ SER ANEXADA AO TR QUE SERÁ INSERIDO NO SEI

MATRIZ DE RISCOS - AQUISIÇÃO

Objeto de Aquisição: CONVERSÃO DE SISTEMAS MAINFRAME PARA PLATAFORMA LINUX x86

Identificação do Risco					Avaliação dos Riscos Probabilidade x Impacto				Planejamento de Resposta aos Riscos		
							Nível do Risco				
Código do Risco	Descrição do Risco	Consequências	Data (Identificação)	Quem identificou o risco	Probabilidade da Ocorrência	Impacto do Risco	Valor	Classificação	Estratégia de resposta	Ações/Resposta	Responsabilidade
1	Interrupção no projeto, causada por indisponibilidade do recurso humano alocado à atividade	Comprometimento do prazo, com impacto nos custos e imagem da Prodeb	06/02/2020	Equipe Técnica	Baixa	Moderado	6,00	Médio	Reduzir	Incluir no termo de referência clausulas que garantam a continuidade dos serviços mesmo em caso de falta do recurso alocado.	Compartilhada
2	Não cumprimento da prestação do serviço contratado, devido à baixa qualificação técnica da equipe do fornecedor	Impacto nos prazos e qualidade das entregas do projeto	06/02/2020	Equipe Técnica	Baixa	Moderado	6,00	Médio	Evitar	Assegurar a qualificação do fornecedor através de requisitos técnicos com as especificações necessárias; Validar os atestados de capacidade técnica durante o processo licitatório.	Compartilhada
3	Entrega fora dos padrões de qualidade exigidos, devido a qualificação técnica dos prestadores	Baixa qualidade do produto, comprometendo o desempenho ou mesmo funcionalidade	06/02/2020	Equipe Técnica	Baixa	Moderado	6,00	Médio	Reduzir	Assegurar a qualificação do fornecedor através da comprovação dos requisitos com as especificações técnicas solicitadas; Fiscalizar e acompanhar as entregas, notificando imediatamente a contratada caso se constate a não conformidade.	Compartilhada
4	Comprometimento do saldo do contrato, decorrente de demanda não prevista e/ou não planejada	Impacto nos prazos e risco à conclusão de etapas do projeto	06/02/2020	Equipe Técnica	Muito Baixa	Grande	4,00	Baixo	Reduzir	Dimensionar adequadamente o saldo e cronograma de pagamentos x entregas no cronograma físico/financeiro. Fiscalizar e acompanhar a evolução do consumo, adotando providências em caso de desvios que comprometam a disponibilidade de saldo atual	Contratante
5	Uso de programas não autorizados ou ilegais por parte dos prestadores de serviço	Pode acarretar na aplicação de sanções e/ou multas de acordo com o contrato estabelecido.	06/02/2020	Equipe Técnica	Muito Baixa	Pequeno	2,00	Baixo	Evitar	Incluir clausulas no termo de referência quanto ao uso de software e aderencia à política de segurança da informação do Estado.	Compartilhada
6	Solução fornecida não aderente aos requisitos ou apresenta falhas	Deficiência no funcionamento da solução, com impacto em prazos, custos e imagem para a Prodeb	06/02/2020	Equipe Técnica	Baixa	Moderado	6,00	Médio	Evitar	Incluir etapa de prova de conceito para avaliação da solução proposta, mediante critérios mínimos estabelecidos, no termo de referência	Contratante
7	Documentação da solução inexistente ou incompleta	Dificuldade na manutenção e operação da solução por parte da equipe PRODEB	06/02/2020	Equipe Técnica	Baixa	Pequeno	4,00	Baixo	Evitar	Incluir clausulas específicas quanto à elaboração da documentação desde o processo de conversão até a documentação do ambiente de suporte aos sistemas convertidos Validar documentação recebida verificando todos os passos/pontos necessários para manter a operação da solução.	Contratante
8	Acompanhamento não adequado do projeto de conversão	Atraso na execução do projeto	06/02/2020	Equipe Técnica	Média	Moderado	9,00	Médio	Evitar	Garantir a alocação de um gerente de projeto do fornecedor para acompanhamento semanal do projeto junto ao gerente de projeto Prodeb.	Compartilhada
9	Acompanhamento não adequado do projeto de conversão	Atraso na execução do projeto	06/02/2020	Equipe Técnica	Média	Moderado	9,00	Médio	Reduzir	Fiscalizar e acompanhar a evolução do projeto, adotando providências caso ocorram desvios na execução do cronograma.	Contratante

O modelo deste documento é de propriedade da Prodeb

Emitido em: 19/02/2020

ANEXO I.I - TR SAQUE DA ATA

Cia. de Processamento de Dados do Estado da Bahia Avenida 4, nº 410, Centro Administrativo da Bahia – CAB Tel. (71) 3115-7611 Fax (71) 3371-5787 CEP 41.745-002 CNPJ 13.579.586/0001-32 Insc. Estadual 70.695.593 Caixa Postal 678 Salvador - Bahia - Brasil www.prodeb.ba.gov.br

PRODEB
TECNOLOGIA, INFORMAÇÃO E SEGURANÇA.

DOCUMENTO PARA ABERTURA DE PROCESSO - DAP

SAQUE DA ATA DE REGISTRO DE PREÇOS Nº 004/2024

---

1. OBJETO

Adesão à Ata de Registro de Preços nº 004/2024, decorrente do Pregão Eletrônico nº 006/2024, para contratação de soluções de segurança incluindo Next-Generation Firewalls (NGFW), soluções para Endpoints, Email, Autenticação de Múltiplos Fatores (MFA) e Honeypot contemplando serviços de implantação, suporte, garantia e serviços continuados gerenciados de segurança da informação, além da prestação de serviços gerenciados continuados englobando operação, atendimento de requisições, gestão de incidentes e vulnerabilidades e monitoramento das soluções de segurança já existentes implantadas no datacenter PRODEB.

2. JUSTIFICATIVA DA AQUISIÇÃO/CONTRATAÇÃO

A Companhia de Processamento de Dados do Estado da Bahia (PRODEB), tem a finalidade de prover serviços de Tecnologia da Informação e Comunicação (TIC) aos órgãos e entidades da Administração Pública e ao setor privado.

Diante do constante avanço tecnológico e da crescente oferta de serviços digitais à população, o Governo do Estado, por meio da PRODEB, tem direcionado investimentos significativos na área de Segurança da Informação. A disponibilização de novas plataformas digitais tem trazido inúmeras facilidades aos cidadãos, no entanto, esse cenário também acompanha uma preocupação com a proteção dos usuários e dados, devido ao aumento proporcional da exposição e do risco de ataques cibernéticos, representando uma ameaça à integridade dos dados sensíveis dos cidadãos e à continuidade dos serviços públicos.

Nesse contexto, a PRODEB tem adotado uma abordagem contundente e proativa, buscando implementar medidas de segurança avançadas e robustas para proteger a infraestrutura tecnológica do Estado e garantir a segurança das informações. Isso inclui a utilização de tecnologias de ponta, a realização de auditorias de segurança regulares, a implementação de políticas e controle de acesso, além do constante aprimoramento das práticas de segurança cibernética, visando mitigar os riscos, preservar o sigilo, a integridade e a disponibilidade das informações.

Essas tecnologias que foram adquiridas nos últimos anos pela Companhia exigem um grande esforço nos quesitos de monitoramento, gerenciamento e administração, e portanto, justificam a contratação de uma empresa especializada para realizar os serviços profissionais especializados e multidisciplinares para o monitoramento e proteção do ambiente de datacenter da PRODEB, garantindo a segurança e a integridade dos dados e sistemas da organização.

Diante de um cenário cada vez mais desafiador em termos de ameaças cibernéticas, a implementação de uma abordagem proativa e abrangente para a segurança da informação torna-se imprescindível. Essa contratação, ao proporcionar uma gama de serviços como gestão de vulnerabilidades, gestão de incidentes e simulações de ataques, possibilitará não apenas a detecção e resposta a incidentes, mas também a identificação e mitigação de possíveis falhas de segurança antes que possam ser exploradas.

A avaliação inicial do ambiente, utilizando um framework reconhecido como o MITRE ATT&CK, permitirá uma análise detalhada dos controles de segurança existentes, oferecendo insights valiosos para aprimoramento contínuo. A supervisão contínua da equipe garantirá a conformidade com as melhores práticas de segurança, além de promover a otimização dos processos e procedimentos operacionais.

Além disso, a capacidade de monitoramento constante e a implementação de controles de acesso robustos contribuirão significativamente para a minimização de riscos, assegurando que somente usuários autorizados tenham acesso ao ambiente sensível do datacenter. A automação e integração das soluções de segurança, bem como a resposta ágil a incidentes, permitirão uma operação mais eficiente e eficaz, reduzindo o impacto potencial de qualquer ameaça.

Portanto, a contratação dos Serviços Profissionais de Monitoramento e Segurança do Datacenter da PRODEB pelo período de 24 Meses é justificada, não apenas pela necessidade de proteção do patrimônio digital da PRODEB, mas também pela constante busca de excelência em segurança da informação, garantindo a continuidade dos serviços e a confiança dos usuários e parceiros.

Cia. de Processamento de Dados do Estado da Bahia Avenida 4, nº 410, Centro Administrativo da Bahia – CAB Tel. (71) 3115-7611 Fax (71) 3371-5787 CEP 41.745-002 CNPJ 13.579.586/0001-32 Insc. Estadual 70.695.593 Caixa Postal 678 Salvador - Bahia - Brasil www.prodeb.ba.gov.br

3. DESCRIÇÃO DETALHADA

Item	Descrição	Qtde	Preço Mensal Ata 004/2024	Preço Total (24 meses) Ata 004/2024
09	Serviços Profissionais de Monitoramento e Segurança do Datacenter da PRODEB pelo período de 24 Meses	1	R$ 380.000,00	R$ 9.120.000,00

Valor total de **R$ 9.120.000,00 (nove milhões, cento e vinte mil reais)**.

4. JUSTIFICATIVA DE PREÇOS

Considerando que os valores constantes na ata de registro de preços, referente ao item 09 - Serviços Profissionais de Monitoramento e Segurança do Datacenter da Prodeb, foram reajustados a menos de 90 dias, conforme consta no Processo SEI n° 065.10933.2024.0010814-61, tendo sido aplicado o percentual de 14,60675% (Catorze virgula sessenta mil seiscentos e setenta e cinco por cento) para redução do preço originalmente registrado, esta gerência entende que não será necessária a realização de nova pesquisa de preços no mercado.

Salientamos que o valor mensal originalmente registrado, de R$ 445.000,00 (quatrocentos e quarenta e cinco mil reais) mensais, após aplicação do percentual de redução, passa a ser de R$ 380.000,00 (trezentos e oitenta mil reais), conforme aditivo n° 002, firmado em 26/11/2024.

5. INFORMAÇÕES SOBRE O ORÇAMENTO

O orçamento a ser utilizado para a contratação pleiteada será o de 2025, pois não haverá faturamento em 2024, mesmo que o saque seja realizado ainda este ano. Isso ocorre porque, conforme descrito no item 4.3 do Termo de Referência (Implantação e homologação dos serviços do item 09), o serviço só será faturado 30 dias após a emissão do Termo de Homologação, que deve ocorrer em até 90 dias após a emissão da Ordem de Serviço.

Custeio (X) Investimento ( )

7. PRAZO PARA ÍNICIO DO SERVIÇO

Os Serviços Profissionais de Monitoramento e Segurança do Datacenter da PRODEB terão início em até 10 (dez) dias úteis após a emissão da Ordem de Serviço pela CONTRATANTE, conforme descrito no item 4.3. IMPLANTAÇÃO E HOMOLOGAÇÃO DOS SERVIÇOS DO ITEM 09.

8. VIGÊNCIA CONTRATUAL

O Contrato terá prazo de vigência de 28 (vinte e oito) meses, a partir da data de assinatura até o limite de 60 (sessenta) meses, conforme previsto no art. 164, do Regulamento de Licitações e Contratos da PRODEB.

9. LOCAL DA EXECUÇÃO DO SERVIÇO

Os serviços serão realizados de forma remota e presencialmente na sede da CONTRATANTE, situada na Avenida 4, nº 410, Centro Administrativo da Bahia – CAB, Salvador, Bahia, CEP: 41.745-002.

10. CONDIÇOES DE PAGAMENTO

Os pagamentos referentes à prestação de serviços prevista no item 09 descrito no TR, serão realizados mensalmente, pelo período em 24 (vinte e quatro) meses, a iniciar em até 30 dias após a emissão do Termo de Homologação.

11. GESTOR E FISCAL DO CONTRATO

Para a gestão e fiscalização do contrato será adotado o rito previsto no Capítulo V, Seção III, do Regulamento de Licitações e Contratos da PRODEB, e designados os seguintes funcionários para os encargos que a gestão implica:

O Gestor para o contrato será o Sr. Antônio Carlos Andrade Borges Junior - Gerência de Tecnologia e Conectividade (GTC), matrícula nº - 92060794, telefone: (71) 3115-7604, E-mail: antonio.borges@prodeb.ba.gov.br

O Fiscal para o contrato será o Sr. Fabricio de Souza Pinto, Coordenador de Suporte a Rede, Matrícula nº 65002945, telefone: (71)3115-7670, e-mail fabricio.pinto@prodeb.ba.gov.br

12. SUBCONTRATAÇÃO

É vedada a subcontratação total ou parcial do objeto.

13. GARANTIA CONTRATUAL

Por ocasião da assinatura do contrato, a empresa vencedora do certame deverá prestar garantia de 5% (cinco por cento) do valor do contrato, podendo optar por uma das modalidades previstas no Regulamento de Licitações e Contratos da PRODEB, ficando esclarecido que a garantia deverá ter seu valor atualizado nas mesmas condições do contrato.

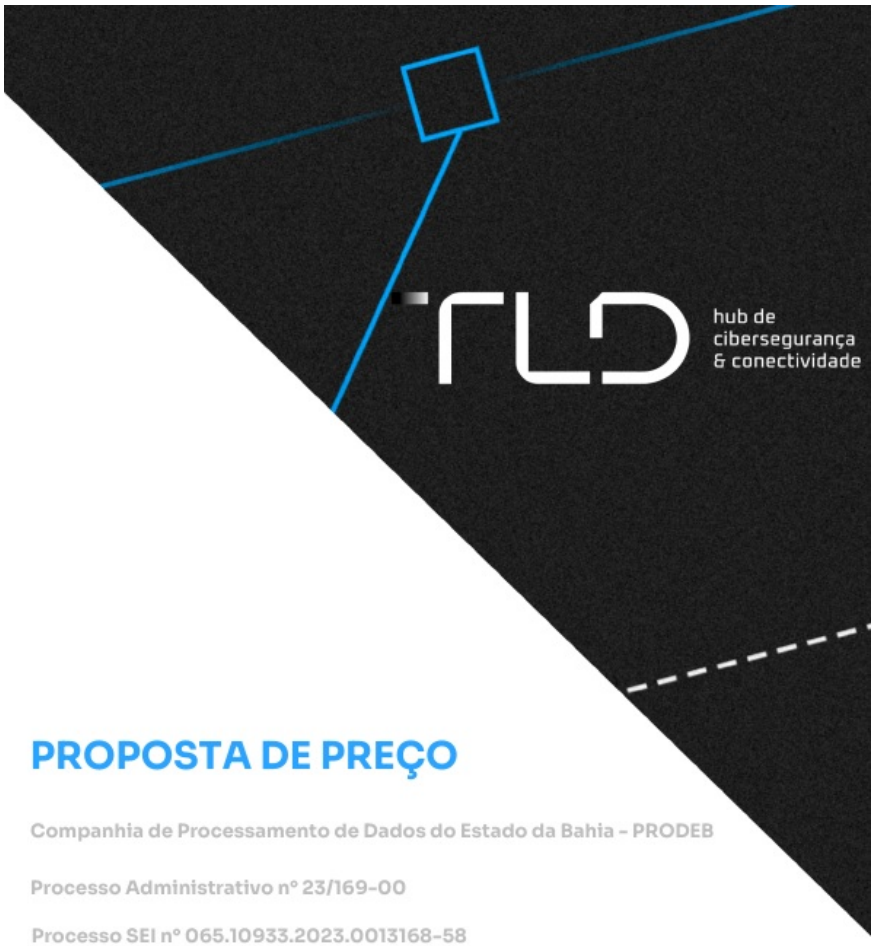
Salvador, 22 de novembro de 2024

Fabricio de Souza Pinto
Coordenador de Suporte à Rede - COSUR

De Acordo,

Antônio Carlos Andrade Borges Junior
Gerente de Tecnologia e Conectividade - GTC

ANEXO II – PROPOSTA DA CONTRATADA



PROPOSTA DE PREÇO

Companhia de Processamento de Dados do Estado da Bahia – PRODEB

Processo Administrativo nº 23/169-00

Processo SEI nº 065.10933.2023.0013168-58

Pregão Eletrônico nº 006/2024

hub de
cibersegurança
& conectividade

1. OBJETO E PREÇO

A TLD TeleData Comércio e Serviços Ltda, inscrita no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda CNPJ/MF sob nº33.927.849/0001-64, Inscrição Estadual sob nº 27.323.346, com sede no município de Salvador, Estado da Bahia, na Rua Sd. Luiz Gonzaga das Virgens, 111 - Edf. Liz Corporate, 4ºandar, sala 402 – Caminho das Árvores, Telefone (71) 3343-3400, e-mail teledata@tld.com.br, por meio deste documento encaminha sua Proposta de Preço, ciente e de acordo com todas as especificações e condições do Termo de Referência, vem, por intermédio do seu representante legal ao final assinado, propor os seguintes preços:

1.1 Objeto:

Contratação de empresa especializada em Tecnologia da Informação e Comunicação (TIC) para fornecimento de soluções de segurança incluindo Next-Generation Firewalls (NGFW), soluções para Endpoints, Email, Autenticação de Múltiplos Fatores (MFA) e Honeypot contemplando serviços de implantação, suporte, garantia e serviços continuados gerenciados de segurança da informação, além da prestação de serviços gerenciados continuados englobando operação, atendimento de requisições, gestão de incidentes e vulnerabilidades e monitoramento das soluções de segurança já existentes implantadas no datacenter PRODEB.

1.2 Preços:

ITENS DE SOFTWARE E HARDWARE						
ITEM	**DESCRITIVO**	**MARCA / SKU**	**DESCRIÇÃO**	**QTD**	**Valor Unit**	**Valor Total**
01	ITEM 01 - Solução de Segurança de Endpoint - EPP	FORTINET / FC1-10-EMS04-429-01-24	Endpoint-based Licenses - EPP/APT (On Premise Deployments) FortiClient EPP/APT Subscription for 25 endpoints, Includes VPN/ZTNA Agent, EPP/APT, on-prem EMS with FortiCare Premium. **Velocidade das portas** = Não se aplica por ser licença de software.	2500	R$ 4.560,00	R$ 11.400.000,00
02	ITEM 02 - Solução para duplo Fator de Autenticação - TokenMobile	FORTINET / FTM-ELIC-5	FortiTokenMobile (Electronic License) Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5 users. Electronic license certificate. **Velocidade das portas** = Não se aplica por ser licença de software.	750	R$ 1.945,00	R$ 1.458.750,00
03	ITEM 03 - Solução de Segurança de Rede NGFW TIPO I	FORTINET / FG-60F	FortiGate-60F 10 x GE RJ45 ports (including 7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port). **Velocidade das portas** = Interfaces 1 x USB Port, 1 x Console Port, 2 x 1GE RJ45 WAN Ports, 1 x 1GE RJ45 DMZ Port, 2 x 1GE RJ45 FortiLink Ports, 5 x 1GE RJ45 Internal Ports.	450	R$ 11.982,00	R$ 5.391.900,00
		FORTINET / (2) FC-10-0060F-950-02-12	FortiGate-60F 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)			
04	ITEM 04 - Solução de Segurança de Rede NGFW TIPO II	FORTINET / FG-VM04V	FortiGate-VM04V FortiGate-VM virtual appliance designed for all supported platforms - 4 x vCPU cores and unlimited RAM. No VDOM by default.	60	R$ 132.761,00	R$ 7.965.660,00
		FORTINET / (2) FC-10-FG4VM-963-02-12	FortiGate-VM04V 1 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)			
		DELL-R450	Servidor PowerEdge R450, Processador Intel Xeon Silver 4309Y 2.8G, 32GB RAM, 4 x Discos de 4TB , 3 anos de garantia ProSupport Plus 24x7. **Velocidade das portas** = Interfaces 1 micro USB iDRAC Direct dedicada, 1 x USB 3.0 interno, 1 x VGA Frontal, 1 x USB 2.0, 1 x porta Ethernet do iDRAC, 1 x USB 3.0 interno, 2 x portas 1G Ethernet RJ45, 1 x VGA.			

05	ITEM 05 - Solução de Segurança de Aplicações WAF TIPO I	FORTINET / FWB-VM04	FortiWeb-VM04 Web Application Firewall - virtual appliance for all supported platforms. Supports up to 4 x vCPU core	8	R$ 380.529,00	R$ 3.044.232,00
		FORTINET / (2) FC-10-VVM04-581-02-12	FortiWeb-VM04 1 Year Advanced Bundle (FortiCare Premium plus AV, FortiWeb Security Service, IP Reputation, FortiSandbox Cloud Service, Credential Stuffing Defense Service and Threat Analytics)			
		DELL-R450	Servidor PowerEdge R450, Processador Intel Xeon Silver 4309Y 2.8G, 32GB RAM, 4 x Discos de 4TB , 3 anos de garantia ProSupport Plus 24x7. **Velocidade das portas** = Interfaces 1 micro USB iDRAC Direct dedicada, 1 x USB 3.0 interno, 1 x VGA Frontal, 1 x USB 2.0, 1 x porta Ethernet do iDRAC, 1 x USB 3.0 interno, 2 x portas 1G Ethernet RJ45, 1 x VGA.			
06	ITEM 06 - Solução de Segurança de Aplicações WAF TIPO II	FORTINET / FWB-VM16	FortiWeb-VM16 Web Application Firewall - virtual appliance for all supported platforms. Supports up to 16 x vCPU core	2	R$ 1.330.938,00	R$ 2.661.876,00
		FORTINET / (2) FC-10-VVM16-581-02-12	FortiWeb-VM16 1 Year Advanced Bundle (FortiCare Premium plus AV, FortiWeb Security Service, IP Reputation, FortiSandbox Cloud Service, Credential Stuffing Defense Service and Threat Analytics)			
		DELL-R550	Servidor Rack PowerEdge R550, Intel® Xeon® Silver 4314 (2.4 GHz, 16 núcleos/32 threads), 96GB RAM, 800GB SSD SAS ISE, 2TB Hard Drive SATA, Broadcom Dual port 10 GbE BaseT **Velocidade de Portas Interfaces** = 1x porta iDRAC dedicada (Micro-AB USB), 1x USB 2.0, 1x VGA Frontal, 1x USB 2.0, 1x porta Ethernet do iDRAC, 1x USB 3.0 interno, 1x VGA, 2x portas 1G Ethernet RJ45, 2x Ethernet 10G			
07	ITEM 07 - Solução de Segurança Decoy/Honeypot	FORTINET / (10) FC1-10-DCVMS-496-02-12	FortiDeceptor-VM Subscription License VM model FortiCare Premium, Deceptor Bundle Contract included license for Deception Decoys, Deception Lures plus FortiGuard Services Subscriptions (ARAE, AV, IPS, and Web Filtering). 1 network VLAN unit price, minimum order of 2 VLANs. Support up to 20 Deception VMs and up to 128 network VLANS	4	R$ 218.304,00	R$ 873.216,00
		FORTINET / (2) LIC-FDC-WIN	FortiDeceptor Windows License Expands FortiDeceptor Licensed Windows VM capacity by 2. (1) Win7 and (1) Win10 license added.			
		DELL-R450	Servidor PowerEdge R450, Processador Intel Xeon Silver 4309Y 2.8G, 32GB RAM, 4 x Discos de 4TB , 3 anos de garantia ProSupport Plus 24x7. **Velocidade das portas** = Interfaces 1 micro USB iDRAC Direct dedicada, 1 x USB 3.0 interno, 1 x VGA Frontal, 1 x USB 2.0, 1 x porta Ethernet do iDRAC, 1 x USB 3.0 interno, 2 x portas 1G Ethernet RJ45, 1 x VGA.			
08	ITEM 08 - Solução de Segurança de Email	FORTINET / FML-3000F	FortiMail-3000F Email Security Appliance - 4 x GE RJ45 ports, 2 x GE SFP slots, 2 x 10GE SFP+ slots, dual AC power supplies, 4TB HDD Default Storage **Velocidade das portas=** 4x 10/100/1000 Interfaces (Copper, RJ45), 2x SFP Gigabit Ethernet Interface, 2x SFP+ 10 Gigabit Ethernet Interface	2	R$ 960.533,00	R$ 1.921.066,00
		FORTINET / (2) FC-10-FE3KF-641-02-12	FortiMail-3000F 1 Year FortiCare Premium and FortiGuard Enterprise ATP Bundle Contract			
		FORTINET / (2) FC-10-FE3KF-409-02-12	FortiMail-3000F 1 Year Cloud Email API Integration service (Microsoft 365 and Google)			
					VALOR TOTAL AQUISIÇÃO (A)	**R$ 34.716.700,00**
					(Trinta e quatro milhões, setecentos e dezesseis mil e setecentos reais.)	

ITENS DE SERVIÇO						
ITEM	DESCRITIVO	SKU	DESCRIÇÃO	QTD	Valor Unit Mensal	Valor Total Mensal
09	ITEM 09 - Serviços Profissionais de Monitoramento e Segurança do Datacenter da PRODEB pelo período de 24 Meses.	SUPORTE	Serviços Profissionais de Monitoramento e Segurança do Datacenter da PRODEB pelo período de 24 Meses em total consonância com as características gerais detalhadas no item 3.9 do Termo de Referência. Em atendimento ao apresentado, o serviço considera a utilização das soluções e produtos instalados e descritos no ANEXO III e para o pleno atendimento aos requisitos de serviços solicitados, é objeto da oferta o complemento com as soluções... Picus Security - complete Security Posture Bundle I Includes all attack modules (Network Infiltration, Email, Web Application, Endpoint, Data Exfiltration). Vendor-specific mitigations. Bu-3-T2; BeyoundTrust Privileged Remote Access Per Named User Cloud (PRAU-CLOUD) & Advanced Web Access (PRA Cloud) (PRA-CLOUD-WEB); e FortiRecon.	1	R$380.000,00	R$ 380.000,00
10	ITEM 10 - Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Endpoint - EPP" para cada item monitorado pelo período de 24 Meses.	SUPORTE	Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Endpoint - EPP" para cada item monitorado pelo período de 24 Meses em total consonância com as características gerais detalhadas no item 3.10 do Termo de Referência	62500	R$ 5,20	R$ 325.000,00
11	ITEM 11 - Serviços Profissionais de Monitoramento e Segurança para o item "Solução para duplo Fator de Autenticação - Token Mobile" para cada item monitorado pelo período de 24 Meses.	SUPORTE	Serviços Profissionais de Monitoramento e Segurança para o item "Solução para duplo Fator de Autenticação - Token Mobile" para cada item monitorado pelo período de 24 Meses em total consonância com as características gerais detalhadas no item 3.11 do Termo de Referência	3750	R$ 7,30	R$ 27.375,00
12	ITEM 12 - Serviços Profissionais de Monitoramento e Segurança para os itens "Solução de Segurança de Rede NGFW TIPO I, II" para cada item monitorado pelo período de 24 Meses.	SUPORTE	Serviços Profissionais de Monitoramento e Segurança para os itens "Solução de Segurança de Rede NGFW TIPO I, II" para cada item monitorado pelo período de 24 Meses em total consonância com as características gerais detalhadas no item 3.12 do Termo de Referência.	510	R$ 650,00	R$ 331.500,00

13	ITEM 13 - Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Aplicações WAF TIPO I e II" para cada item monitorado pelo período de 24 Meses.	SUPORTE	Serviços Profissionais de Monitoramento e Segurança para o item "Solução de Segurança de Aplicações WAF TIPO I, II" para cada item monitorado pelo período de 24 Meses em total consonância com as características gerais detalhadas no item 3.13 do Termo de Referência.	8	R$ 7.150,00	R$ 57.200,00
VALOR TOTAL MENSAL SERVIÇOS (B) PAGAMENTO MENSAL						**R$ 1.121.075,00**
VALOR TOTAL PARA 24 MESES (C) VALOR TOTAL MENSAL SERVIÇOS (B) X 24 (vinte e quatro) MESES						**R$ 26.905.800,00**
VALOR GLOBAL DO LOTE VALOR TOTAL AQUISIÇÃO (A) + VALOR TOTAL PARA 24 MESES (C)						**R$ 61.622.500,00**
(sessenta e um milhões, seiscentos e vinte e dois mil quinhentos reais)						

1.3. Origem de Fabricação dos equipamentos

Itens 01,02,03 e 08 -Fortinet - 1570 Atlantic Street, Union City, CA 94587, USA.
Itens 04,05,06,07 – Fortinet - 1570 Atlantic Street, Union City, CA 94587, USA. e Servidores Dell - Av. da Emancipação, 5000 - Parque dos Pinheiros, Hortolândia - SP, CEP: 13184-654

2. CONDIÇÕES COMERCIAIS

2.1 Garantia e Suporte Técnico

A garantia técnica, suporte e de licenciamento do software serão de 24 (vinte e quatro) meses, com cobertura de atendimento on-site e profissionais especializados com o objetivo de manter em perfeito estado de operação os serviços e equipamentos, tais como: no que tange ao hardware: desinstalação, reconfiguração ou reinstalação decorrentes de falhas no hardware, fornecimento de peças de reposição, substituição de hardware, atualização da versão de drivers, firmwares e software básico, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados; e no que tange a software: desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados. Deve ser incluído correções, "patches", "fixes", "updates", "service packs", novas "releases", "versions", "builds", "upgrades", englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia técnica especificado;

A manutenção técnica corretiva será realizada por meio da abertura de chamado (sem limitação de quantidade), via telefone, Internet, e-mail e/ou website e somente poderá ser fechado após a confirmação do Solicitante responsável, a partir da disponibilidade do recurso para uso em perfeitas condições de funcionamento. Na abertura de chamados técnicos, serão enviadas informações como: número de série e código do equipamento, anormalidade observada, nome do responsável pela solicitação do serviço, versão do software utilizada no hardware, severidade do chamado e ao final será apresentado relatório contendo identificação do chamado, data e hora da sua abertura, data e hora do início e término do atendimento, identificação do defeito, técnico responsável pela solução, as providências adotadas e outras informações pertinentes. Este relatório será homologado pelo gestor do contrato PRODEB.

Contato para atendimento e Suporte:
Contratada:
Serviço de Atendimento ao Cliente:
Página Web: http://teledata.desk.ms
Telefone: 0800-000-0594
E-mail: servicedesk@tld.com.br

Para substituição de peças, utiliza-se o serviço de RMA (Return Merchandise Authorization ou Retorno de Mercadoria Avariada, em português) com envio de equipamentos em até 36 horas úteis, licenciado pelo período de 24 (vinte e quatro) meses. Caso seja impossível a substituição dos equipamentos, componentes, materiais ou peças por outras que não as que compõem o item proposto, esta substituição obedecerá ao critério de compatibilidade, que poderá ser encontrado no site do fabricante, através de equivalência e semelhança, e só poderá ser efetuada mediante expressa autorização da PRODEB, para cada caso particular. Caso a PRODEB recuse o equipamento, componente, material e ou peça a ser substituído, serão apresentadas alternativas, sem alteração no prazo para solução do problema.

Ao fim do contrato de garantia e licenciamento, a solução permanece funcional, capaz de criar, customizar e gerenciar políticas e regras, gerar e encaminhar logs, manipular dashboard e entre outras funções necessárias ao manuseio da solução, exceto para funcionalidades que dependam de serviços hospedados em nuvem.

2.1.1 Níveis Mínimos de Serviço (Serviços Profissionais de Monitoramento e Segurança):

Os Serviços Profissionais de Monitoramento e Segurança serão prestados no regime (24x7) vinte e quatro horas por dia, sete dias por semana, pelo período da contratação, para os tipos de atendimentos discriminados a seguir:

INCIDENTES OPERACIONAIS			
SEVERIDADE	**DESCRIÇÃO**		
1- CRÍTICA	A solução de segurança não está operante e não é possível nenhuma solução de contorno viável. Problema na solução que gera indisponibilidade em sistemas/serviços produtivos que dependem desse ativo.		
2- ALTA	Problema na solução de segurança que gera impacto em determinado sistema/serviço produtivo que dependem desse ativo.		
3 - MÉDIA	Problema contornável que não gera qualquer impacto aos sistemas/serviços produtivos que dependem desses ativos.		
4 - BAIXA	Consultas técnicas e dúvidas sobre as soluções de segurança		
SEVERIDADE	**PRAZO DE ATENDIMENTO**		
	TMIA	**TMSO**	**TMSD**
1- CRÍTICA	15 min	2h	24h
2- ALTA	30 min	4h	48h
3 - MÉDIA	1 h	8h	72h
4 - BAIXA	2h	16h	144h
LEGENDA			
TMIA	Tempo máximo para início de atendimento: Tempo máximo requerido para o início do atendimento;		
TMSO	Tempo máximo para solução operacional: Tempo máximo de recuperação, ou seja, tempo requerido para contornar o problema e deixar a solução/sistema/serviço disponível;		
TMSD	Tempo máximo para solução definitiva do chamado: Tempo máximo requerido para solucionar em definitivo a causa do problema;		

REQUISIÇÕES		
SEVERIDADE	**DESCRIÇÃO**	
1- CRÍTICA	Requisições que impactam diretamente na segurança e integridade dos serviços/sistemas considerados críticos no portfólio da CONTRATANTE, ameaçam a continuidade dos serviços ou representam riscos iminentes.	
2- ALTA	Requisições que têm um impacto significativo, mas não imediatamente crítico. Podem afetar operações importantes ou serviços que não são considerados como críticos no portfólio da CONTRATANTE.	
3 - MÉDIA	Requisições que afetam operações ou usuários de forma limitada, sem impacto imediato nos serviços essenciais.	
4 - BAIXA	Requisições que têm baixo impacto operacional, geralmente tarefas de manutenção preventiva, geração de relatórios, consultas ou informações não críticas	
SEVERIDADE	**PRAZO DE ATENDIMENTO**	
	TMIA	**TMSO**
1- CRÍTICA	15 min	2h
2- ALTA	30 min	4h
3 - MÉDIA	1 h	8h
4 - BAIXA	2h	16h
LEGENDA		
TMIA	Tempo máximo para início de atendimento: Tempo máximo requerido para o início do atendimento;	
TMS	Tempo máximo para solução: Tempo máximo requerido para solucionar a requisição;	

RESPOSTA A INCIDENTES DE SEGURANÇA			
SEVERIDADE	**DESCRIÇÃO**		
1- CRÍTICA	Incidentes com níveis de risco crítico ou vulnerabilidades consideradas como críticas, identificadas pelas soluções de segurança, probabilidade de materialização ou com materialização confirmada de risco de impacto crítico que poderia afetar a operação da CONTRATANTE, como um ataque cibernético que cause uma indisponibilidade em qualquer serviço		
2- ALTA	Incidentes com níveis de risco alto ou vulnerabilidades consideradas como altas, identificadas pelas soluções de segurança, probabilidade de materialização ou com materialização confirmada de risco de impacto alto que poderia afetar a operação da CONTRATANTE, como um ataque cibernético que cause uma degradação em qualquer serviço		
3 - MEDIA	Incidentes com possível materialização de risco de impacto moderado ou vulnerabilidades consideradas como médias, como uso inadequado de recursos tecnológicos ou configurações incorretas que precisam ser ajustadas		
4 - BAIXA	Este nível de severidade é aplicado para solicitação de configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento dos serviços contratados ou equipamentos fornecidos		
SEVERIDADE	**PRAZO DE ATENDIMENTO**		
	TMIR	**TMCI**	**TMR**
1- CRÍTICA	15 min	2h	24h
2- ALTA	30 min	4h	48h
3 - MEDIA	1h	8h	72h
4 - BAIXA	2h	16h	144h
LEGENDA			
TMIA	Tempo máximo para início de resposta: Tempo máximo requerido para o início da resposta ao incidente de segurança		
TMCI	Tempo máximo de contenção do incidente: Tempo máximo contenção do incidente de segurança;		
TMR	Tempo máximo de resposta ao incidente: Tempo máximo requerida identificação, contenção e mitigação ou proposição de mitigações do incidente de segurança;		

2.2 Prazo de Entrega / Execução:

O prazo de entrega dos equipamentos e licenças dos itens são de até 60 (sessenta) dias, a partir da assinatura do contrato, obedecendo o cronograma a seguir:

Equipamentos e Licenças

Itens: 01 a 08

ATIVIDADES	PRAZO
Início do planejamento para elaboração do Plano de Instalação, Configuração, migração e demais ações conjunto com a CONTRATANTE dos Itens 01 a 08	Até 10 dias após a assinatura do contrato
Prazo de Entrega dos Equipamentos (Itens 01 a 08) e hands-on do produto.	Até 60 dias a partir da assinatura do contrato
Recebimento Provisório dos Equipamentos e Licenças	Até 05 dias após Entrega dos Equipamentos
Recebimento Definitivo dos Equipamentos testados em funcionamento e licenças ativadas com a validade solicitada no TR	Até 05 (cinco) dias úteis após o recebimento provisório
Início da Instalação da Solução	Até 15 dias após o recebimento definitivo
Conclusão da Instalação da Solução	Até 10 dias após Início da Instalação da Solução
Entrega da Documentação Final	Até 10 dias após Conclusão da Instalação, Configuração
Resolução de Inconformidades	Até 05 dias após validação inicial da CONTRATANTE
Emissão do Termo de Homologação	Até 10 dias após entrega da Documentação Final sem inconformidades

Referente ao item: 09

ATIVIDADES	PRAZO
Início do planejamento para elaboração do do Plano de Implantação em conjunto com a CONTRATANTE	Até 5 (cinco) dias após a emissão da Ordem de Serviço
Apresentação dos relatórios da avaliação do ambiente e diagnóstico inicial das vulnerabilidades existentes da CONTRATANTE	Até 30 dias após a emissão da Ordem de Serviço
Implementação do Centro de Operações	Até 60 dias após a emissão da Ordem de Serviço
Conclusão da ativação do Serviço do Monitoramento	Conforme cronograma definido no Plano de Implantação
Início da execução do Plano de Testes para validação da solução	5 dias úteis após a conclusão da ativação do serviço
Execução do Plano de Testes para validação da solução	10 dias úteis após seu início
Início do Período de Funcionamento Experimental – PFE	2 dias úteis após a conclusão do plano de testes
Fim do Período de Funcionamento Experimental – PFE	10 dias úteis após seu início
Entrega da Documentação Final e Relatório de Linha Base	Até 10 dias após Conclusão do Fim do Período de Funcionamento Experimental – PFE
Resolução de Inconformidades	Até 03 dias após acionamento da CONTRATANTE
Emissão do Termo de Homologação	Até 10 dias após entrega da Documentação Final
Emissão da primeira nota fiscal	30 dias após a emissão do Termo de Homologação

Referente aos Itens: 10 a 13

ATIVIDADES	PRAZO
Início do planejamento para elaboração do do Plano de Implantação em conjunto com a CONTRATANTE	Até 5 (cinco) dias após a emissão da Ordem de Serviço
Conclusão da ativação do Serviço de Monitoramento	Conforme cronograma definido no Plano de Implantação
Entrega da Documentação Final	Até 10 dias após Conclusão da Ativação
Resolução de Inconformidades após Termo de Homologação	Até 03 dias após acionamento da CONTRATANTE
Emissão do Termo de Homologação	Até 10 dias após entrega da Documentação Final
Emissão da primeira nota fiscal	30 dias após a emissão do Termo de Homologação

2.2 Local de Entrega:

ITENS 01, 02, 03, 04 e 05	Na unidade Sede, situada na Região Metropolitana de Salvador, em dias úteis, nos horários: • Segunda a quinta: 08:00hs às 12:00hs e das 13:30hs às 17:30hs; • Sexta: 08:00hs às 12:00hs e das 13:30hs às 16:00hs.
ITENS 06, 07 e 08	Na unidade Sede da PRODEB, situada na Avenida 4, nº 410, CAB, Salvador, nos horários: • Segunda a quinta: 08:00hs às 12:00hs e das 13:30hs às 17:30hs • Sexta: 08:00hs às 12:00hs e das 13:30hs às 16:00h

2.3 Pagamento:

O pagamento referente aos itens 01 ao 08, serão realizados em parcela única após a emissão do Termo de Homologação que caracteriza a entrega e instalação das soluções;

O pagamento referente as prestações de serviços dos itens 09 ao 13, serão realizados de mensalmente, pelo período em 24 (vinte e quatro) meses, com início 30 (trinta) dias após a emissão do Termo de Homologação, que caracteriza a finalização da implantação e operação dos serviços;

Conforme o art. 10, do Regulamento de Licitações e Contratos da PRODEB, o prazo para pagamento é de acordo com o valor dos bens adquiridos, a saber:

Até R$ 50.000,00, até 15 (quinze) dias; | Até R$ 100.000,00, até 30 (trinta) dias; | Demais valores, até 45 (quarenta e cinco) dias;

2.4 Vigência do Contrato: O Contrato terá prazo de vigência de 28 (vinte e oito) meses, a partir da data de assinatura.

2.5 Vigência da Ata de Registro: A vigência da Ata será de 12 (doze) meses, a contar da data de sua assinatura.

2.6 Validade da Proposta: A proposta de preços tem validade de 60 (sessenta) dias a contar da data da sessão pública.

2.7 Demais Despesas: Nos preços ofertados estão contempladas todas e quaisquer despesas necessárias ao fiel cumprimento do objeto desta licitação, inclusive 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.

2.8 Os equipamentos ofertados são novos, de primeiro uso e na última versão de hardware e software disponíveis no mercado. Além disso, os equipamentos e softwares não constam, na presente data, em listas de end-of-sale, end-of-support, end-of-life ou similares do fabricante.

2.9 A descrição da proposta de preços atende integralmente ao disposto no Edital e Termo de Referência.

2.10 Declaramos que temos conhecimento e concordamos com todos os itens mencionados no Termo de Referência, documento base para a presente proposta de preços.

3. DADOS PARA ASSINATURA DO CONTRATO

NOME COMPLETO	Ricardo Luiz de Oliveira
RG	735283826
CPF	684.548.135-00
CARGO	CEO

4. DADOS DA PROPONENTE

Razão Social: TLD TeleData Comércio e Serviços Ltda
CPNJ: 33.927.849/0001-64
Endereço: Rua Sd. Luiz Gonzaga das Virgens, 111 – Edf. Liz Corporate, 4º andar, sala 402 – Caminho das Árvores, Cep: 41.820-560, Salvador – BA

Contatos: Marcelle Hora / Matheus Serrado
Telefones: (71) 3343-3439 / (71) 3343-3441 / (71) 98823-9953 / (71) 98146-0933
E-mail: servicedesk@tld.com.br / contratos@tld.com.br / faturamento@tld.com.br
Representante Legal: Ricardo Luiz de Oliveira
CPF: 684.548.135-00
E-mail: ricardo@tld.com.br
Banco: Bradesco Agência: 1425 Conta: 41288-0

Na expectativa de sermos distinguidos com suas prezadas ordens, estamos a inteira disposição de V.S.as. para quaisquer esclarecimentos adicionais que se façam necessários.

Salvador, 06 de novembro de 2024.

TLD TeleData Comércio e Serviços Ltda.
CNPJ.: 33.927.849/0001-64
Ricardo Luiz de Oliveira
R.G. nº 735283826-SSP/BA- CPF.: 684.548.135-00
CEO

ANEXO III - MATRIZ DE RISCOS

PRODEB

COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DA BAHIA

*ESTA PLANILHA DEVERÁ SER ANEXADA AO TR QUE SERÁ INSERIDO NO SEI

MATRIZ DE RISCOS - AQUISIÇÃO

Objeto de Aquisição:	CONVERSÃO DE SISTEMAS MAINFRAME PARA PLATAFORMA LINUX x86

Identificação do Risco					Avaliação dos Riscos Probabilidade x Impacto				Planejamento de Resposta aos Riscos		
							Nível do Risco				
Código do Risco	Descrição do Risco	Consequências	Data (Identificação)	Quem identificou o risco	Probabilidade da Ocorrência	Impacto do Risco	Valor	Classificação	Estratégia de resposta	Ações/Resposta	Responsabilidade
1	Interrupção no projeto, causada por indisponibilidade do recurso humano alocado à atividade	Comprometimento do prazo, com impacto nos custos e imagem da Prodeb	06/02/2020	Equipe Técnica	Baixa	Moderado	6,00	Médio	Reduzir	Incluir no termo de referência clausulas que garantam a continuidade dos serviços mesmo em caso de falta do recurso alocado.	Compartilhada
2	Não cumprimento da prestação do serviço contratado, devido à baixa qualificação técnica da equipe do fornecedor	Impacto nos prazos e qualidade das entregas do projeto	06/02/2020	Equipe Técnica	Baixa	Moderado	6,00	Médio	Evitar	Assegurar a qualificação do fornecedor através de requisitos técnicos com as especificações necessárias; Validar os atestados de capacidade técnica durante o processo licitatório.	Compartilhada
3	Entrega fora dos padrões de qualidade exigidos, devido a qualificação técnica dos prestadores	Baixa qualidade do produto, comprometendo o desempenho ou mesmo funcionalidade	06/02/2020	Equipe Técnica	Baixa	Moderado	6,00	Médio	Reduzir	Assegurar a qualificação do fornecedor através da comprovação dos requisitos com as especificações técnicas solicitadas; Fiscalizar e acompanhar as entregas, notificando imediatamente a contratada caso se constate o não cumprimento da qualidade	Compartilhada
4	Comprometimento do saldo do contrato, decorrente de demanda não prevista e/ou não planejada	Impacto nos prazos e risco à conclusão de etapas do projeto	06/02/2020	Equipe Técnica	Muito Baixa	Grande	4,00	Baixo	Reduzir	Dimensionar adequadamente o saldo e cronograma de pagamentos x entregas no cronograma físico/financeiro. Fiscalizar e acompanhar a evolução do consumo, adotando providências em caso de desvios que comprometam a disponibilidade de saldo atual	Contratante
5	Uso de programas não autorizados ou ilegais por parte dos prestadores de serviço	Pode acarretar na aplicação de sanções e/ou multas de acordo com o contrato estabelecido.	06/02/2020	Equipe Técnica	Muito Baixa	Pequeno	2,00	Baixo	Evitar	Incluir clausulas no termo de referência quanto ao uso de software e aderência à política de segurança da informação do Estado.	Compartilhada
6	Solução fornecida não aderente aos requisitos ou apresenta falhas	Deficiência no funcionamento da solução, com impacto em prazos, custos e imagem para a Prodeb	06/02/2020	Equipe Técnica	Baixa	Moderado	6,00	Médio	Evitar	Incluir etapa de prova de conceito para avaliação da solução proposta, mediante critérios mínimos estabelecidos, no termo de referência	Contratante
7	Documentação da solução inexistente ou incompleta	Dificuldade na manutenção e operação da solução por parte da equipe PRODEB	06/02/2020	Equipe Técnica	Baixa	Pequeno	4,00	Baixo	Evitar	Incluir clausulas específicas quanto à elaboração da documentação desde o processo de conversão até a documentação do ambiente de suporte aos sistemas convertidos Validar documentação recebida verificando todos os passos/pontos necessários para manter a operação da solução.	Contratante
8	Acompanhamento não adequado do projeto de conversão	Atraso na execução do projeto	06/02/2020	Equipe Técnica	Média	Moderado	9,00	Médio	Evitar	Garantir a alocação de um gerente de projeto do fornecedor para acompanhamento semanal do projeto junto ao gerente de projeto Prodeb.	Compartilhada
9	Acompanhamento não adequado do projeto de conversão	Atraso na execução do projeto	06/02/2020	Equipe Técnica	Média	Moderado	9,00	Médio	Reduzir	Fiscalizar e acompanhar a evolução do projeto, adotando providências caso ocorram desvios na execução do cronograma.	Contratante

ANEXO IV - TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Os abaixo-assinados, de um lado a **COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DA BAHIA - PRODEB** , CNPJ nº 13.579.586/0001-32, situada na cidade de SALVADOR, à AVENIDA QUATRO, Nº 410 – CENTRO ADMINISTRATIVO DA BAHIA, doravante denominada CONTRATANTE, e de outro lado o **CONSÓRCIO CYBERSEC BAHIA**, CNPJ nº55.904.689/0001-70, situada na Rua Soldado Luiz Gonzaga das Virgens, 111, Edf. Liz Corporate, andar 4, Caminho das Árvores, Salvador/BA, CEP 41.820-560, doravante denominada CONTRATADA, têm entre si justa e acertada, a celebração do presente TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE, através do qual a CONTRATADA aceita não divulgar sem autorização prévia e formal segredos e informações sensíveis de propriedade da CONTRATANTE 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 compartilhadas com 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 qualquer 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 24/136-01, deverá entregar à CONTRATANTE todo e qualquer material de propriedade desta, inclusive notas pessoais envolvendo matérias sigilosas relacionadas com a CONTRATANTE, 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 coleta dos Termos de Sigilo de seus colaboradores não exime a CONTRATADA das penalidades por violação das regras por parte de seus contratados.

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 seguir a 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 24/136-01, 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___.

_____

COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DA BAHIA

_____

CONSÓRCIO CYBERSEC BAHIA

ANEXO V – GARANTIA

Documento assinado eletronicamente por **João Gualberto Rizzo Araújo**, **Representante Legal da Empresa**, em 11/12/2024, às 20:27, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014 .

Documento assinado eletronicamente por **Ricardo Luíz de Oliveira**, **Representante Legal da Empresa**, em 11/12/2024, às 21:06, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014 .

Documento assinado eletronicamente por **Carlos Augusto Borges Silva**, **Diretor**, em 12/12/2024, às 09:05, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014 .

Documento assinado eletronicamente por **Alexandre Rodrigo Cruz Rios Corujeira de Britto** , **Usuário Externo**, em 12/12/2024, às 09:49, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014 .

Documento assinado eletronicamente por **Jose Muniz Reboucas**, **Diretor Executivo**, em 12/12/2024, às 17:33, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014 .

A autenticidade deste documento pode ser conferida no site https://seibahia.ba.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **00104616368** e o código CRC **306F80ED**.