GOVERNO DO ESTADO DA BAHIA
Secretaria do Trabalho, Emprego, Renda e Esporte
COORDENAÇÃO DE CONTRATOS E CONVÊNIOS - SETRE/GAB/DG/CONTRATOS

CONTRATO Nº 016/2025

MODALIDADE DE LICITAÇÃO	NÚMERO
PREGÃO ELETRÔNICO - REGISTRO DE PREÇO	006/2024

CONTRATO QUE ENTRE SI CELEBRAM O ESTADO DA BAHIA, POR INTERMÉDIO DA SECRETARIA DO TRABALHO, EMPREGO, RENDA E ESPORTE E O CONSÓRCIO CYBERSEC BAHIA, PARA OS FINS QUE NELE SE DECLARAM

O **ESTADO DA BAHIA**, por intermédio da **SECRETARIA DO TRABALHO, EMPREGO, RENDA E ESPORTE - SETRE**, CNPJ nº 13.937.123/0001-03, situada à Av. Luiz Viana Filho, 200, 3ª Plataforma, 2ª Avenida, Centro Administrativo da Bahia – CAB, CEP: 41.745-003, Salvador-BA, neste ato representado pelo seu titular, **Sr. AUGUSTO SÉRGIO VASCONCELOS DE OLIVEIRA**, brasileiro, portador da cédula de identidade RG nº. 837604745 SSP/BA e do CPF nº 798.142.985-49, autorizado pelo Decreto Simples publicado no D.O.E. de 10/01/2025, doravante denominado **CONTRATANTE**, e o **CONSÓRCIO CYBERSEC BAHIA**, CNPJ n o 55.904.689/0001-70, situada à Rua Soldado Luiz Gonzaga das Virgens, 111, Edf. Liz Corporate, andar 4, Caminho das Árvores, Salvador/BA, CEP 41.820-560, constituido pelas empresas: **TLD HUB DE CIBERSEGURANÇA & CONECTIVIDADE LTDA.**,CNPJ nº 33.927.849/0001-64, situada na Rua Soldado Luiz Gonzaga das Virgens nº 111 – Sala 402 – Caminho das Árvores, Salvador/BA, CEP 41.820-560, **empresa líder do consórcio, constituída através do Instrumento de Constituição de Consórcio, Cláusula Nona**, anexo V deste Instrumento e **CENTRO DE PESQUISAS EM INFORMÁTICALTDA**, CNPJ nº 40.584.096/0001-05, situada na Rua Edistio Ponde, nº 353, Edif. Empresarial Tancredo Neves, Salas 807 e 808. Stiep. Salvador/ BA, CEP 41.770-395, neste ato representadas pelos Srs. **RICARDO LUIZ DE OLIVEIRA**, portador da Carteira Nacional de Habilitação nº 02914186355, inscrito no CPF/MF sob o no684.548.135-00 e **ALEXANDRE RODRIGO CRUZ RIOS CORUJEIRA DE BRITTO**, portador da Carteira Nacional de Habilitação nº 02495532572, inscrito no CPF/MF sob o nº 411.255.335-87, adjudicatária do **RP/ PE PRODEB** nº 006/2024, processo administrativo no **065.10933.2023.0013168-58,** conforme Ata do Registro de Preço e Autorização, que integram este Instrumento na qualidade de anexos III e IV respectivamente, doravante denominado sem conjunto **CONTRATADA**, celebram o presente contrato, nos termos do Processo SEI nº. **021.2142.2024.0005465-03,** que se regerá pela Lei Estadual nº 9.433/05, pelas normas gerais da Lei Federal nº 8.666/93, sua srespectivas alterações, na forma do §1º, art.2º do Decreto Estadual nº 22.416 de 01 de dezembro de 2023 e conforme disposição prevista no §2º do Art. 2º do Decreto Estadual nº22.416/2023, mediante as cláusulas e condições a seguir ajustadas:

CLÁUSULA PRIMEIRA–OBJETO

Constitui objeto do presente contrato 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 do Termo de Referência do instrumento convocatório e da proposta apresentada pela CONTRATADA, que integram este instrumento na qualidade de Anexos I e II, respectivamente.

§1º A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem no objeto, de até 25% do valor inicial atualizado do contrato, na forma dos §1º e 2º do art. 143 da Lei estadual no 9.433/05.

§2º As supressões poderão ser superiores a 25%, desde que haja resultado de acordo entre os contratantes.

§3º É vedada a subcontratação parcial do objeto, a associação da CONTRATADA com outrem, a cessão ou transferência, total ou parcial do contrato, não se responsabilizando o CONTRATANTE por nenhum compromisso assumido por aquela com terceiros.

CLÁUSULA SEGUNDA–PRAZO

O prazo de vigência do contrato, a contar da data da sua assinatura, será de **28 (vinte e oito) meses**, admitindo-se a sua prorrogação para o iten 1, os serviços do iten 10, nos termos do inc. II do art. 140 da Lei estadual no 9.433/05.

§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 por meio de termo aditivo, devendo o pedido ser realizado no prazo máximo de 60 (sessenta) dias antes do término do contrato.

CLÁUSULA TERCEIRA–GARANTIA

A garantia contratual será de 5% do valor do contrato, podendo recair sobre qualquer das modalidades previstas no §1º do art. 136 da Lei estadual nO 9.433/05.

§1º Sob pena da caracterização de inadimplemento contratual, a prova da garantia, na hipótese de opção pela modalidade caução em dinheiro ou títulos da dívida pública, deverá ser apresentada no prazo máximo de 05 (cinco)diascontados da data de assinatura do contrato,admitindo-se, para o seguro-garantia e a fiança bancária, que a comprovação seja feita no prazo máximo de 30 (trinta) dias daquela data, sem o que fica vedada, em qualquer caso, a realização de pagamento.

§2º A garantia responderá pelo inadimplemento das obrigações contratuais e pelas multas impostas,independentemente de outras cominações legais.

§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 deferidopara a comprovação da garantia originária, visando assegurar a cobertura das modificações procedidas.

§6º Será recusada a garantia que não atender às especificações solicitadas, devendo ser notificada a CONTRATADA para que, no prazo de 05 (cinco) dias, sane a incorreção apontada ou, no caso de títulos da dívida pública, seguro-garantia ou fiança bancária, promova a substituição por caução em dinheiro.

§7º O retardamento, a falta da apresentação ou a não substituição da garantia impedirá a realização do pagamento das faturas apresentadas, sem prejuízo da incidência de multa moratória, da rescisão do contrato nos termos do art. 167, inc. III, da Lei no9.433/05 e das demais cominações legais.

§8º A devolução da garantia ocorrerá após o recebimento definitivo da totalidade do objeto do contrato, com a demonstração de cumprimento, pela CONTRATADA, das obrigações pactuadas.

CLÁUSULA QUARTA–REGIME DE EXECUÇÃO

Serviço com empreitada por preço global

CLÁUSULA QUINTA–PREÇO

O CONTRATANTE pagará à CONTRATADA pelos serviços efetivamente prestados os valores abaixo especificados:

ITENS DE SOFTWARE E HARDWARE / ITENS DE SERVIÇO					
ITEM	**DESCRITIVOS**	**UNID**	**QTD**	**VALORUNITARIOMENSAL**	**VALORTOTALMENSAL**
01	**SOLUCAO DE SEGURANCA DE ENDPOINT - EPP** - Com garantia, suporte e licenciamento por 24 meses. Permite a instalação, gerenciamento e atualizações para 25 endpoints, com administração remota via console central. Inclui funcionalidade Zero Trust, tuneis criptografados, e licenciamento para AI Powered NGAV, Cloud Sandbox, Automated Endpoint Quarantine, Application Firewall e Application Inventory. Suporta sistemas operacionais Windows Desktop, Windows Server, MAC OS, Android, Linux, apresenta interface gráfica multilingue, backup de configuração, geração de logs e controle de acesso a dispositivos removíveis. Possuem recursos avançados de analise cooperativa, antivírus, firewall de aplicativos, VPN IPSEC e SSL. Proporciona visibilidade detalhada, analise de vulnerabilidades, filtro de conteúdo web com categorização dinâmica de sites e políticas de acesso baseadas em expressões regulares. As funcionalidades abrangem provisionamento de clientes, notificações pop-up, e analise continua para manter a integridade e seguranca do ambiente de Endpoint	UN	**44**	**R$ 4.560,00**	**R$ 200.640,00**
10	**SERVICOS DE CONFIGURACAO**, administracao,operacao, atendimento a mudancas e requisicoes, aplicacao de melhores praticas do fabricante e monitoramento para a solucao de Endpoint Protection especificada no item Servicos Profissionais de Mnonitoramento e Seguranca para o item Solucao de Seguranca de Endpoint - EPP para cada item monitorado pelo periodo de 24 meses	UN	**1100**	**R$ 124,80**	**R$137.280,00**
VALOR TOTAL DO CONTRATO				**R$ 337.920,00**	

§1º Estima-se para o contrato o valor global de **R$337.920,00** (trezentos e trinta e sete mil e novecentos e vinte reais)

§2º 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

CLÁUSULA SEXTA–DOTAÇÃO ORÇAMENTÁRIA

As despesas para o pagamento deste contrato correrão por conta dos recursos da Dotação Orçamentária a seguir especificada:

UNIDADE ORÇAMENTÁRIA	**FONTE/BA**	**PAOE**	**NATUREZA DA DESPESA**	**UNIDADE GESTORA**
3.21.101 – APG	0.100	2002	33.90.30.000 33.90.40.000	0003 – DA
3.21.602 - FET/BA	0.100	2002	33.90.30.000 33.90.40.000	0001 - FET/BA

CLÁUSULA SÉTIMA–OBRIGAÇÕES DA CONTRATADA

A CONTRATADA, além das determinações contidas no instrumento convocatório, bem como daquelas decorrentes de lei, obriga-se a:

I. designar de sua estrutura administrativa um preposto permanentemente responsável pela perfeita execução do contrato, inclusive para atendimento de emergência, servindo de interlocutor e canal de comunicação entre as partes;

II. executar o objeto deste contrato de acordo com as especificações técnicas constantes do instrumento convocatório e do presente contrato, nos locais, dias, turnos e horários determinados;

III. manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e recursos humanos para execução completa e eficiente do objeto deste contrato;

IV. zelar pela boa e completa execução dos serviços contratados e facilitar, por todos os meios ao seu alcance, a ampla açãofiscalizadora dos prepostos designados pelo CONTRATANTE, atendendo prontamente às observações e exigências que lhe forem solicitadas;

V. comunicaraoCONTRATANTEqualqueranormalidadequeinterfiranobomandamentodosserviços;

VI. atender com presteza as reclamações sobre a qualidade dos serviços executados, providenciando sua imediata correção, sem ônus para o CONTRATANTE;

VII. respeitar e fazer com que seus empregados respeitem as normas de segurança do trabalho, disciplina e demais regulamentos vigentes no CONTRATANTE, bem como atentar para as regras de cortesia no local onde serão executados os serviços;

VIII. 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;

IX. arcar com todo e qualquer dano ou prejuízo de qualquer natureza causado ao CONTRATANTE e terceiros, porsua culpa, ou em conseqüência de erros, imperícia própria ou de auxiliares que estejam sob suaresponsabilidade, bem como ressarcir o equivalente a todos os danos decorrentes de paralisação ou interrupção dos serviços contratados, exceto quando isto ocorrer por exigência do 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;

X. manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, inclusive de apresentar, ao setor de liberação de faturas e como condição de pagamento, os documentos necessários;

XI. providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes, necessários à execução dos serviços;

XII. 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;

XIII. adimplir os fornecimentos exigidos pelo instrumento convocatório e pelos quais se obriga, visando à perfeita execução deste contrato;

XIV. emitirnotasfiscais/faturasdeacordocomalegislação;

XV. observaralegislaçãofederal,estadualemunicipalrelativaaoobjetodocontrato;

XVI. executarosserviçossemsoluçãodecontinuidadedurantetodooprazodavigênciadocontrato;

XVII. proverasinstalações,aparelhamentoepessoaltécnicoexigidosnalicitação;

XVIII. alocar durante todo o período de execução do objeto a equipe técnica mínima exigida no instrumento convocatório,admitindo-seasuasubstituiçãoporprofissionaisdeexperiênciaequivalenteousuperior,desdeque aprovada pelo CONTRATANTE.

XIX. providenciaro cadastramento deseurepresentantelegalou procuradorno site www.comprasnet.ba.gov.br, para a prática de atos através do Sistema Eletrônico de Informações – SEI.

Parágrafo único. Além das determinações acima descritas, a CONTRATADA que estiver sujeita à determinação do art. 429 do Decreto-Lei nO 5.452, de 1Ode maio de 1943 (Consolidação das Leis do Trabalho - CLT), regulamentado pelo Decreto nO5.598, de 1º de dezembro de 2005, deverá, no que concerne à aprendizagem:

a) recrutar, preferencialmente, para a contratação de aprendizes prevista no art. 429 da CLT, os estudantes indicados nos incisos I e II do art. 9Oda Lei estadual nO13.459, de 10 dezembro de 2015, regulamentada pelo Decreto estadual nO16.761, de 07 de junho de 2016, no percentual mínimo de 20% (vinte por cento) do quadro de aprendizes da **CONTRATADA**;

b) apresentar ao fiscal ou responsável pela gestão e acompanhamento do contrato, no prazo de até 05 (cinco) dias úteis contado do início efetivo da execução do serviço, a lista completa dos aprendizes, indicando aqueles selecionados no banco de dados de que trata o Decreto estadual nO16.761/16, devendo justificar, perante o CONTRATANTE, a eventual impossibilidade de seu cumprimento.

CLÁUSULA OITAVA–OBRIGAÇÕES DO CONTRATANTE

O **CONTRATANTE,**alémdasobrigaçõescontidasnestecontratopordeterminaçãolegal,obriga-sea:

I. forneceràCONTRATADAoselementosindispensáveisaocumprimento docontrato noprazomáximo de 10(dez) dias da assinatura;

II. realizaropagamentopelaexecuçãodoobjetocontratual;

III. proceder à publicação resumida do instrumentodecontrato edeseus aditamentos, na imprensaoficial,no prazo legal.

CLÁUSULA NONA–FISCALIZAÇÃO DO CONTRATO

Competirá ao CONTRATANTE proceder ao acompanhamento da execução do contrato, na forma do art. 154 da Lei estadual no9.433/05, ficando esclarecido que a ação ou omissão, total ou parcial da fiscalização não eximirá a CONTRATADA da total responsabilidade pela execução do contrato.

§1º O adimplemento da obrigação contratual por parte da CONTRATADA ocorrerá com a efetiva prestação do serviço,a realização da obra, a entrega do bem ou de parcela destes, bem como qualquer outro evento contratual cuja ocorrência esteja vinculada à emissão de documento de cobrança, nos termos do art. 8o, inc. XXXIV, da Lei estadual no 9.433/05.

§2º Cumprida a obrigação pela CONTRATADA, caberá ao 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 art. 154, inc. V, e art. 155, inc. V, da Lei estadual no9.433/05.

§3º Compete especificamente à fiscalização, sem prejuízo de outras obrigações legais ou contratuais:

I. exigirdaCONTRATADAocumprimentointegraldasobrigaçõespactuadas;

II. rejeitartodoequalquermaterialdemáqualidadeounão especificado;

III. relataraoGestordoContratoocorrênciasoucircunstânciasquepossamacarretardificuldadesnodesenvolvimento dos serviços em relação a terceiros;

IV. dar à autoridade superior imediata ciência de fatos que possam levar à aplicação de penalidades contra a CONTRATADA ou mesmo à rescisão do contrato.

V.

§4º Fica indicada como a área responsável pela gestão do contrato: COORDENAÇÃO DE SUPORTE, INFRAESTRUTURA E MANUTENÇÃO TIC (CMA)

§5º Fica indicado como gestor deste Contrato a servidora: Elanne Santana Monteiro, Matricula: 21.479.860-9

§6º Fica indicado como fiscal deste Contrato o servidor: Marcio Eduardo Brito Gomes, matricula – 92127019 e os servidores membros da Comissão de Fiscalização de Contratos nomeados através da Portaria 096/2019

CLÁUSULA DÉCIMA–RECEBIMENTO DO OBJETO

O recebimento do objeto, consistente na aferição da efetiva prestação do serviço, realização da obra, entrega do bem ou de parcela destes, se dará segundo o disposto no art. 161 da Lei estadual no9.433/05, observando-se os seguintes prazos, se outros não houverem sido fixados no Termo de Referência:

I. 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;

II. 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.

§1º Nos casos de aquisição de equipamentos de grande vulto, o recebimento definitivo far-se-á mediante termo circunstanciado e, nos demais, mediante recibo.

§2º Na hipótese de não ser lavrado o termo circunstanciado ou de não ser procedida a verificação dentro dos prazos fixados,reputar-se-ão comorealizados, desdeque comunicado sao CONTRATANTE nos15(quinze) dias anteriores à exaustão dos mesmos

§3º O recebimento definitivo de compras ou serviços, cujo valor do objeto seja superior ao limite estabelecido para a modalidade de convite, deverá ser confiado a uma comissão de, no mínimo, 03 (três) membros.

§4º Esgotado o prazo de vencimento do recebimento provisório sem qualquer manifestação do CONTRATANTE, não dispondo o TERMO DE REFERÊNCIA de formadiversa, considerar-se-á definitivamente aceito pela Administração o objeto contratual, para todos os efeitos.

§5º Poderá ser dispensado o recebimento provisório nos seguintes casos:

I. gêneros perecíveis e alimentação preparada;

II. serviços profissionais;

III. serviços de valor até o limite previsto para compras e serviços, que não sejam de engenharia, namodalidade de convite, desde que não se componham de aparelhos, equipamentos e instalações sujeitos à verificação de funcionamento e produtividade.

§6º Salvo disposiçõesemcontrárioconstantesdo TERMO DE REFERÊNCIA, osensaios,testese demaisprovasexigidas por normas técnicas oficiais para a boa execução do objeto do contrato correm por conta do contratado.

§7º O CONTRATANTE rejeitará, no todo ou em parte, obra, serviço ou fornecimento em desacordo com as condições pactuadas, podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis.

§8º O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança da obra ou do serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo contrato.

§9º Com a conclusão da etapa do recebimento definitivo, a CONTRATADA estará habilitada a apresentar as nota(s) fiscal(is)/fatura(s) para pagamento.

CLÁUSULA DÉCIMA–PRIMEIRA-PAGAMENTO

Os pagamentos devidos à CONTRATADA serão efetuados através de ordem bancária ou crédito em conta~~corrente~~aberta em instituição financeira contratada pelo Estado da Bahia, no prazo não superior a 08 (oito) dias úteis, contados dadatadaapresentaçãodafatura,apósconcluídoorecebimentodefinitivo,emconsonânciacomodispostonoart.6o,

§5o;art.8o,XXXIV;art.79,XI,"a";art.154,Veart.155,VdaLeiestadualno9.433/05.

§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, indicativo da satisfação pela CONTRATADA de todas as obrigações pertinentes ao objeto contratado.

§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 O CONTRATANTE descontará da fatura mensal o valor correspondente às faltas ou atrasos no cumprimento da obrigação, com base no valor do preço vigente.

§4º A(s) nota(s) fisca(l)is/fatura(s) deverá(ao) atender as exigências legais pertinentes aos tributos e encargos relacionados com a obrigação,sujeitando-se às retenções tributárias previstas em lei, e, as situações específicas,à adoção da forma eletrônica.

§5º O processo de pagamento, para efeito do art. 126, inciso XVI, da Lei estadual no9.433/05, deverá ser instruído com a prova da manutenção das condições de habilitação e qualificação exigidas no certame, o que poderá ser aferido mediante consulta ao Registro Cadastral ou a sites oficiais, considerando-se como marco final desta demonstração a data de conclusão da etapa do recebimento definitivo.

§6º Emhavendo alguma pendênciaimpeditiva do pagamento, a exemplode erro na apresentação danota fiscal/fatura ou dos documentos pertinentes à contratação, ou, ainda, de 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 o CONTRATANTE.

§7º EmcasodemoranospagamentosdevidospeloCONTRATANTE,seráobservadooquesesegue:

I. a atualização monetária 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;

II. nas compras para entrega imediata, assim entendidas aquelas com prazo de entrega até 15 (quinze) dias contados da data da celebração do ajuste, será dispensada a atualização financeira correspondente ao período compreendido entre as datas do adimplemento e a prevista para o pagamento, desde que não superior a quinze dias, em conformidade com o inc. II do art. 82 da Lei no9.433/05.

§8º Optando a CONTRATADA por receber os créditos em instituição financeira diversa da indicada no **caput**, deverá arcar com os custos de transferências bancárias, os quais serão deduzidos dos pagamentos devidos.

CLÁUSULA DÉCIMA-SEGUNDA–MANUTENÇÃO DAS CONDIÇÕES DA PROPOSTA

Ospreçoscontratadossãofixoseirreajustáveisduranteoprazode12mesesdadatadeapresentaçãodaproposta.

§1º Após o prazo de 12 meses a que se refere o caput, a concessão de reajustamento será feita mediante a aplicação do INPC/IBGE, nos termos do inc. XXV do art. 8oda Lei estadual no9.433/05.

§2º A revisãode preços, nos termos do inc. XXVI do art. 8oda Leiestadualno9.433/05, dependerá de requerimento da CONTRATADA quando visar recompor o preço que se tornou insuficiente, devendo ser instruído com a documentação que comprove o desequilíbrio econômico-financeiro do contrato.

§3º 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 no 10.406/02.

§4º A revisão de preços pode ser instaurada pelo CONTRATANTE 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, conforme o art. 143, inc. II, alínea "e", da Lei estadual no9.433/05.

CLÁUSULA DÉCIMA-TERCEIRA–ALTERAÇÕES CONTRATUAIS

Aprorrogação,suspensãoourescisãosujeitar-se-ãoàsmesmasformalidadesexigidasparaavalidadedestecontrato.

§1º A admissão da fusão, cisão ou incorporação da CONTRATADA está condicionada à manutenção das condições de habilitação e à demonstração, perante o CONTRATANTE, da inexistência de comprometimento das condições originariamente pactuadas para a adequada e perfeita execução do contrato.

§2º Independemdetermocontratualaditivo,podendoserregistradoporsimplesapostila:

I. asimplesalteraçãonaindicaçãodosrecursosorçamentáriosouadicionaiscusteadoresdadespesa,sem modificação dos respectivos valores;

II. reajustamento de preços previsto no edital e neste contrato, bem como as atualizações, compensações ou apenações financeiras decorrentes das condições de pagamento dos mesmos constantes;

III. o empenho de dotações orçamentárias suplementares até o limite do seu valor corrigido.

CLÁUSULA DÉCIMA-QUARTA INEXECUÇÃO E RESCISÃO

A inexecução total ou parcialdocontratoensejaráasuarescisão,comasconseqüênciascontratuaiseasprevistasnaLei estadual no9.433/05.

§1º A rescisão poderá ser determinada por ato unilateral e escrito do CONTRATANTE nos casos enumerados nos incisos I a XV, XX e XXI do art. 167 da Lei estadual no9.433/05.

§2º Quando a rescisão ocorrer com base nos incisos Ie XVI a XX do art. 167 da Lei estadual nO 9.433/05, sem que haja culpa da CONTRATADA, será este ressarcido dos prejuízos regularmente comprovados que houver sofrido, na forma do §2º do art. 168 do mesmo diploma.

CLÁUSULA DÉCIMA-QUINTA–PENALIDADES

Constituem ilícitos administrativos as condutas previstas nos arts. 184, 185 e 199 da Lei estadual no9.433/05, sujeitando-se os infratores às cominações legais, especialmente as definidas no art. 186 do mesmo diploma, garantida a prévia e ampla defesa em processo administrativo.

§1º Para a aplicação das penalidades serão levados em conta a natureza e a gravidade da falta, os prejuízos dela advindos para a Administração Pública e a reincidência na prática do ato, observando-se os critérios de dosimetria estabelecidos pelo Decreto estadual no13.967/12.

§2º Serão punidos com a pena de declaração de inidoneidade para licitar e contratar com a Administração, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a autoridade competente para aplicar a punição, os que incorram nos ilícitos previstos nos incisos I a V do art. 184, nos incisos II, III e V do art. 185 e no art. 199 da Lei estadual no9.433/05.

§3º Serão punidos com a pena de suspensão temporária do direito de cadastrar e licitar e impedimento de contratar com a Administração os que incorram nos ilícitos previstos nos incisos VI e VII do art. 184 e nos incisos I, IV, VI e VII do art. 185 da Lei estadual no9.433/05.

§4º A CONTRATADA será descredenciada do Sistema de Registro Cadastral quando, em razão da ocorrência das faltas previstasnaLeiestadualno9.433/05,deixardesatisfazerasexigênciasrelativasà habilitação jurídica, qualificação técnica, qualificação econômico-financeira, regularidade fiscal e trabalhista exigidas para cadastramento.

§5º A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará a CONTRATADA à multademora,naformaprevistanacláusulaseguinte,queserágraduadadeacordocomagravidadedainfração, observado o disposto na Lei estadual no9.433/05 e no Decreto estadual no13.967/12.

CLÁUSULA DÉCIMA-SEXTA–SANÇÃO DEMULTA

A pena de multa será aplicada em função de inexecução contratual, inclusive por atraso injustificado na execução do contrato, sem prejuízo da rescisão unilateral do contrato, a qualquer tempo, e a aplicação das demais sanções previstas na Lei estadual no 9.433/05.

§1º Quanto à obrigaçã oprincipal, será observado o que se segue:

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

II. Caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicado opercentual de 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 ou do serviço já realizado.

III. O atraso no cumprimento da obrigação principal ensejará a aplicação de multa no 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 subseqüente ao trigésimo, calculados sobre o valor da parcela do fornecimento ou do serviço em mora.

§2º Quanto à obrigação acessória, assim considerada aquela que coadjuva a principal, seráobservado o que se segue:

I. Em caso de descumprimento total da obrigação acessória, será a plicada multa no percentual de 10% (dez por cento) incidente sobre o valor ou custo da obrigação descumprida.

II. Caso o cumprimento da obrigação acessória, uma vez iniciado, seja descontinuado, será aplicado o percentual de 5% (cinco por cento) sobre o valor ou custo da obrigação descumprida.

III. Oatrasonocumprimentodaobrigação acessóriaensejaráaaplicação demultanopercentualde0,2% (dois décimos por cento) ao dia, até o trigésimo dia de atraso, e de 0,6% (seis décimos por cento) por cada dia subseqüente ao trigésimo, calculados sobre o valor ou custo da obrigação descumprida.

IV. Caso não seja possível identificar o valor ou custo da obrigação acessória descumprida, a multa será arbitrada pelo CONTRANTE, em valor que não supere 1% da sanção pecuniária que seria cabível pelo descumprimento da obrigação principal.

§3º 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 em lei.

§4o Na hipótese de o contratado se negar a efetuar o reforço da caução, dentro de 10 (dez) dias contados da data de sua convocação, será aplicada multano percentual de 2,5% (dois emeio por cento) incidente sobre o valor global do contrato.

§5o Asmultas previstasnestacláusulanão têmcarátercompensatórioeo seupagamentonãoeximirá aCONTRATADA da responsabilidade por perdas e danos decorrentes das infrações cometidas.

§6o Amulta,aplicadaapósregularprocessoadministrativo,serádescontadadagarantiadocontratadofaltoso.

§7o Se o valor da multa exceder ao da garantia prestada, além da perda desta, a CONTRATADA responderá pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou, ainda, se for o caso, cobrada judicialmente.

§8o Casonãotenhasidoexigidagarantia,àAdministraçãosereservaodireitodedescontardiretamentedo pagamento devido à CONTRATADA o valor de qualquer multa porventura imposta.

CLÁUSULA DÉCIMA-SÉTIMA VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO

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

CLÁUSULA DÉCIMA-OITAVA 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 nO12.290, de 20 de abril de 2011, e do Decreto nO15.805, de 30 de dezembro de 2014.

Parágrafoúnico. ACONTRATADAdeverámanteratualizadooendereçoeletrônicocadastradonoSistemaEletrônicode Informações - SEI, para efeito do recebimento de notificação e intimação de atos processuais.

CLÁUSULA DÉCIMA-NONA–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 deste contrato.

E, por estarem assim justos e contratados, firmam o presente contrato na presença das testemunhas que subscrevem depois de lido e achado conforme.

AUGUSTO SÉRGIO VASCONCELOS DE OLIVEIRA
SECRETARIA DO TRABALHO, EMPREGO, RENDA E ESPORTE – SETRE

RICARDO LUIZ DE OLIVEIRA
CONSÓRCIO CYBERSEC BAHIA

ALEXANDRE RODRIGO CRUZ RIOS CORUJEIRA DE BRITTO
CONSÓRCIO CYBERSEC BAHIA

Testemunhas:

CPF: CPF:

ANEXO ÚNICO - TERMO DE REFERÊNCIA
PREGÃO ELETRÔNICO Nº 006/2024
CONTRATO 016/2025

1. OBJETO DA CONTRATAÇÃO

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 desegurança já existentesimplantadasno datacenter PRODEB.

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;

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.

Os itens 06, 07, 08 e 09 serão consumidos exclusivamente pela Prodeb devido a terem sido planejados para atenderespecificamenteainfraestruturadesegurançainstaladaemseuDataCentereacapacidadeparaatender 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 PoderExecutivodoEstadodaBahia,temafinalidadedeproverserviçosdeTecnologiadaInformaçãoeComunicação –TIC comsegurança,confiabilidadeedisponibilidade,garantindoacontinuidadedosnegócioseaproteçãodasinformaçõesdos 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 meiodaPRODEB,temdirecionadoinvestimentossignificativosnaáreadeSegurançadaInformação.Adisponibilizaçãode 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

implementaçãodepolíticasecontroledeacesso,alémdoconstanteaprimoramentodaspráticasdesegurançacibernética, visando mitigar os riscos, preservar o sigilo, a integridade e a disponibilidade das informações.

Essassoluçõesdesegurança,gerenciadaspelaPRODEB,concentram-senaproteçãodascamadasdeInterneteDatacenter. Noentanto,háumainfraestruturacorporativacomplexaqueinterligatodasasunidadesdosÓrgãosdoGovernodoEstado da Bahia em uma extensa rede privada de comunicação de dados. Essa rede é composta pela Rede Governo III e IV e IDB

(InfoviaDigitaldaBahia)quefuncionamdeformaintegradaepermitequeasunidadessecomuniquementresi,facilitando oacessoaosserviçoseotimizandooprocessosoperacionais.APRODEBatuacomogestoratécnicadessasRedesatuando 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 1milhão 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 RedesLocais (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.

VistoqueosÓrgãosdaAdministraçãoPúblicatêmcomoobjetivoprincipalaprestaçãodeserviçosaocidadão,eparaisso, precisam concentrar seus esforços em suas atividades fim, que são aquelas que estão diretamente relacionadas à sua missão.Sendoassim,paraaprimoraraproteçãoemumníveldemaiorgranularidade,trazendosegurançaparaosdiversos dispositivos conectados, para minimizar o **risco de vazamento** e comprometimento de dados sensíveis e o **risco deindisponibilidade** de serviços essenciais por tempo indeterminado, torna-se de fundamental importância a **aquisição desoluções 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 instaladas 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.

2. DETALHAMENTO DO OBJETO – LOTE ÚNICO

ITENS DE SOFTWARE E HARDWARE			
ITEM	**DESCRITIVO**	**UNID**	**QUANTIDADE**
01	SoluçãodeSegurançadeEndpoint-EPP	UN	2500
02	SoluçãoparaduploFatordeAutenticação-TokenMobile	UN	750
03	SoluçãodeSegurançadeRedeNGFWTIPOI	UN	450
04	SoluçãodeSegurançadeRedeNGFWTIPOII	UN	60
05	SoluçãodeSegurançadeAplicaçõesWAFTIPOI	UN	08
06	SoluçãodeSegurançadeAplicaçõesWAFTIPOII	UN	02
07	SoluçãodeSegurançaDecoy/Honeypot	UN	04
08	SoluçãodeSegurançadeEmail.	UN	02

ITENSDESERVIÇOS			
ITEM	**DESCRITIVO**	**UNID**	**QUANTIDADE**
09	ServiçosProfissionaisdeMonitoramentoeSegurançado Datacenter da PRODEB pelo período de 24 Meses.	UN	1
10	ServiçosProfissionaisdeMonitoramentoeSegurançapara oitem “Solução de Segurança de Endpoint - EPP” para cada item monitoradopeloperíodode24Meses.	UN	62.500
11	ServiçosProfissionaisdeMonitoramentoeSegurançapara oitem “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“SoluçãodeSegurançadeRedeNGFWTIPOI,II”paracada itemmonitoradopeloperíodode24Meses.	UN	510
13	ServiçosProfissionaisdeMonitoramentoeSegurançapara oitem “SoluçãodeSegurançadeAplicaçõesWAFTIPOI”paracada item monitoradopeloperíodode24Meses.	UN	08

3. DETALHAMENTO DAS ESPECIFICAÇÕES TÉCNICAS

ITEM01–SOLUÇÃO DE SEGURANÇA DE ENDPOINT–EPP

Deve permitir a instalação, gerência e atualizações das funcionalidades de 25 (vinte ecinco) endpoints,durante toda vigência contratual 24 (vinte e quatro) meses;

Devepermitir o gerenciamento dosclientesde segurança remotamente, a partir deum consolecentral do próprio fabricante;

DevepossuifuncionalidadeZeroTrustApplied,comtúneiscriptografadosautomáticosparacontroleacesso validado por sessão a aplicativos, através de funcionalidade de avaliação de postura do EndPoint;

Deve estar licenciados com as funcionalidades de AI Powered NGAV, Cloud Sandbox, Automated Endpoint Quarantine, Application Firewall e Application Inventory;

Olicenciamentodevesebasearnonúmerodeclientesregistradosnoconsoledegerenciamentocentraldo mesmo fabricante;

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;

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”

DevesercompatívelcompelosmenososseguintessistemasoperacionaIs:

MicrosoftWindows:7(32e64bits),8(32e64bits),8,1(32e64bits),10(32e64bits)e11(64bits);

MicrosoftWindowsServer:2012,2012R2,2016e2019;

MacOS11+,v10.14,v10.15;

Android5.0esuperiores;

LinuxUbuntu16.04,CentOs7.4;

Deveterumainterfacegráficadousuário,pelomenosnosidiomasinglês,português eespanhol;

Devepermitirobackupdoarquivodeconfiguração;

Devesercapazdegerarumdiário(logs)nasfuncionalidadesinstaladaseconfiguradas;

Deve suportar pelo menos os seguintes níveis de log devem estar disponíveis: emergência, alerta, crítico, erro, aviso, informativo;

Osclientesdesegurançadeverãopoderenviaroslogsparaoservidorconsoledegerenciamentocentral;

OsclientesdesegurançadeverãopermitiraconfiguraçãolocalviaXML(eXtensibleMarkupLanguage);

Os clientes de segurança deverão suportar integração às tecnologias Sandboxing pelo menos do mesmo fabricante;

Deve controlar o acesso a dispositivos removíveis e ser capaz de monitorar, permitir ou negar acesso a dispositivos USB

Devepoderdefinironíveldolog:emergência,alerta,crítico,erro,aviso,aviso,depuração,informações;

Deveterumagentedelogonúnico;

Deveteracapacidadededesabilitarosserviçosdeproxyparaerrosdedepuração;

Deve ser capaz de ativar seletivamente logs em: VPN, Antivírus, Atualizações, Sandboxing, Comunicação com segurança cooperativa, filtro de web e verificação de vulnerabilidade;

Devesuportarexportaroslogsparaforadoclientedesegurança

FUNCIONALIDADESDEANÁLISECOOPERATIVA

Devesercapazdeintegraraumaestruturacooperativaparacompartilharinformaçõesereceber atualizações de assinaturas dinâmicas;

Devesuportaroenviodelogsparaumanalisadorcentraldelogs,ondeosíndicesdecompromissos do (IoC)seja processado (taxas de confirmação)

Deve suportar receber atualizações de assinaturas dinâmicas da solução de proteção avançada de ameaças (ATP) ou sandboxing

Deveserdisponibilizadoumaferramentaquepermitaaaplicaçãodepolíticasdiferentes, independente do cliente estar conectado ou não à rede corporativa;

Devepermitirficaremquarentenanoconsolecentralouemalgumoutrocomponentequefaça parte da solução de segurança cooperativa.

FUNCIONALIDADESDEANTIVÍRUS

Oclientedesegurançadeveteracapacidadedeinspecionararquivosexecutáveis,bibliotecase drivers quanto a vírus;

Oclientedesegurançadevesercapazdeverificaratualizaçõesdeassinaturaautomaticamente

Oclientedesegurançadevesercapazdeenviararquivosparainspeçãonossistemas Sandboxing do mesmo fabricante;

Oclientedesegurançadevesercapazdebloquearoscanaisdecomunicaçãousadosporhackers ou atacantes;

Oclientedesegurançadevenotificarlocalmentequandoumvírusédetectado

Oclientedesegurançadevepermitirqueousuárioinicieumaverificaçãosobdemanda

O cliente de segurança deve permitir que a verificação de vírus seja iniciada automaticamente regularmente

Oclientedesegurançadevepermitiravisualizaçãodosarquivosemquarentena

Devepermitiraconfiguraçãodoperfilantivírusapartirdoconsolecentraldomesmofabricante

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.

A ferramenta de proteção baseada em nuvem NÃO deve enviar o arquivo inteiro ou seus metadados. SOMENTE a soma de verificação

Aferramentadeproteçãobaseadaemnuvemdeveanalisarapenasarquivosdealtorisco,como, entre outros, documentos do Word, Excel, PDF e DLL.

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

Devesercapazdeenviararquivosparaumasoluçãodeproteçãoavançadadeameaças(ATP)(ou sandboxing) antes de ser acessado;

Devesuportarsandboxlocalmenteouatravésdeumasoluçãoemnuvem

Devesercapazdebloquearoacessoaoarquivoatéqueosandboxdêumveredicto

Caso um arquivo seja marcado como malicioso pela Sandbox, o mesmo deve ser mantido em quarentena;

FUNCIONALIDADESDEFIREWALLDEAPLICATIVOS

Oclientedesegurançadevesuportarperfisde ControledeAplicativos,criadoscentralmenteno console de gerenciamento do mesmo fabricante;

Ofabricantedevepermitirqueosclientesdesegurançafaçamconsultason-linesobrea categoria de um determinado aplicativo a ser usado na política de controle de acesso

Devepossuirpelomenos4000aplicativosreconhecidosemsuabaseparaquepossamserusados nas regras de controle de acesso dos clientes de segurança

FUNCIONALIDADESDEVPNIPSEC

DevepermitirqueousuáriocrienovasVPNsIPSEC

DevepermitirqueváriasVPNsIPSECsejamdefinidassimultaneamente

Devepermitiraautenticaçãousandonomedeusuárioesenha

Devepermitiraautenticaçãousandocertificadosdigitais

DevepermitiraseleçãodosmodosPrincipaleAgressivo;

DevepermitiraconfiguraçãodoDHCPporIPSec;

DevepermitirousodoNATTraversal;

Devepermitiraescolhadegrupos Diffie-Hellman(1,2,5e14);

Devepermitirconfiguraçõesdeexpiraçãodechave IKE;

DevesuportarIKEv1eIKEv2

DevepermitirousodoPerfectForwardSecrecy;

Devepermitiraautenticaçãodedoisfatoresfornecidapelomesmofabricante

FUNCIONALIDADESDEVPNSSL

DevepermitirqueousuáriocrienovasVPNsSSL

DevepermitirqueváriasVPNsSSLsejamdefinidassimultaneamente

DevepermitirapersonalizaçãodaportaTCPnaqualaVPNSSLfunciona

Devepermitiraautenticaçãousandonomedeusuárioesenha

Devepermitiraautenticaçãodedoisfatoresfornecidapelomesmofabricante

Devepermitiraautenticaçãousandocertificadosdigitais

ParausoespecíficodeVPNSSL(pelomenos):

EspecificaçãoIPdoconcentrador;

Especificaçãodaportadohub;

DevesuportarousodeautenticaçãoSAML(SecurityAssertionMarkupLanguage)paraos clientes que rodam na plataforma Microsoft Windows.

FUNCIONALIDADESDEGERECIAMENTOCENTRALIZADO

DevepermitirainstalaçãonoMicrosoftWindowsServer2012R2,2016ou2019;

Oconsoledegerenciamentocentralizadodeveserentreguesemcusto;

Devepermitiraadiçãodeclientesadicionandolicenças.

Deveterinterfacegráficadegerenciamento

Deveterfuncionalidadedebackup

Devepermitiracriaçãodeusuáriosdediferentesperfisadministrativos

DevepermitirimportarinformaçõesdoActiveDirectoryusandoLDAP

Devepermitirregistromanualdaestaçãoatravésdeumusodeumasenha

Devepermitiracriaçãodegruposdeclientesparafacilitarogerenciamento

DevepermitirqueaconfiguraçãodoclientemedianteadefiniçõesemXML

Devepermitirqueasconfiguraçõesdeperfilsejamimportadasemumdispositivodefirewalldo mesmo fabricante

Devepermitiraconfiguraçãodediferentesgruposeperfisparafacilitaraadministração

Deve permitir a configuração de antivírus, filtro da web, controle de aplicativos, verificador de vulnerabilidades e perfis de VPN

Devepermitiraproteçãoemtempo real

Devepermitirqueaconfiguraçãodepesquisasdevírusevulnerabilidadesemumabase agendada

Devepermitirverificaçãocompletaeverificaçãorápida

DevepermitirqueousuárioconfigureVPNslocalmente

Devepermitirqueousuáriodesconecteuma VPN

DevepermitiraconexãoVPNantesdologin

DevepermitirconexãoVPNautomática

DevesuportarousoespecíficoougeralparaVPNIPSec(pelomenos)

Devesuportarousodecertificadosouusuárioesenhaparaautenticação

Devesuportarousodecertificadosnocartãointeligente

Devesuportarobloqueiodetráfego IPv6

Devesuportaràopçãoparaousuárioacessaraconfiguraçãodoclienteporsenha

Devesercapazdeenviarlogsparaumsistemadelogexternosdomesmofabricante

Deverpermitirainstalaçãodocertificadodigitalnocliente

DevepermitirativarasfuncionalidadesdeLogonÚnico

Deveterinformaçõesdisponíveissobre:Númerodedispositivosgerenciados,Versãodosistema operacional, Perfil aplicado, Usuário, Versão de assinatura do antivírus

Statusdoclientedesegurança:Registradoounãoregistrado

Deveconterinformaçõessobreosistemaoperacionalnoqualoclienteestáinstalado

Deveinformaroperfildesegurançacriadoe/ouaplicado

Deveinformarosrecursosdesegurançaaplicados:antivírus,filtrodaweb,VPN,firewallde aplicativo;

Devepermitirhabilitaroudesabilitarosrecursosantivírus,filtrodaweb,VPN,firewallde aplicativo nos terminais gerenciados

Devesercapazdefazeruminventáriodosoftwareinstaladoemcadanódeextremidade

Devepermitir a implantação automática declientesdeterminal deacordo com a OU do MS AD ou grupos do MS AD

Deve permitir a manutenção de várias instâncias de instaladores com recursos diferentes (AV, VPN, WF, etc.) e arquiteturas (x86, x64, etc.)

DevepermitiraimplantaçãodeequipamentosqueNÃOpertencemaoactivedirectory(AD)

Devepermitirqueregrasdeconformidadedeficientesimpeçamqueumclientemalconfigurado se conecte a redes críticas

Devesercapazdeseracessadoatravésdaadministração WEB

Deveterumpainelemquepossaverificarrapidamenteostatusdeintegridadedosclientes

Develidarcomlistascentralizadasdequarentenadearquivos

Devepoderaplicarpolíticasaosterminaisdeacordocomosgrupos,paraqueosclientes pertencentes a esse grupo tenham a mesma política.

Devepoderaplicarpolíticasaosterminaisdeacordocomousuáriopertencenteaogrupo, tornando mais granular à aplicação da política.

Deve poderatribuirconfigurações dinamicamente quandoos clientes forem movidos dosgrupos

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 deaplicativos,VPN,verificaçãodevulnerabilidadeseconfigurações dosistema(porexemplo,logfiels)

Os usuários administradores devem poder sincronizar com o AD, para permitir o login com as mesmas credenciais

Devesercapazdedefinirfunçõesadministrativas

Deve suportar fazer backup / restaurar configurações do console, configuração do servidor, políticas de terminal etc.

FuncionalidadesdeProvisionamentodeClientes

O fabricante deve fornecer um portal para baixar a segurança do cliente e permitir a instalação local

DevesercompatívelcomainstalaçãoviaMicrosoftActiveDirectory

O console de gerenciamento central deve poder instalar o cliente de segurança nos computadores Windows associados a um domínio da Microsoft

Devesuportarcriaçãodeváriasversõesdepacotesdeinstalaçãoparaseremassociadasagrupos do Microsoft Active Directory.

VISIBILIDADE

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,Sistemaoperacionale/ousalesforce),statusdocliente,Nomedohost,etiquetade host

Devesuportaruploaddeumafotoouavatarparaidentificaçãorápidadousuário

Deverelatardemaneirarápidaerápida,sefizerpartedeumambientedesegurançacooperativo

Deverelatarrapidamenteoníveldevulnerabilidadedaestaçãodetrabalho

Deveterumsistemadenotificaçãopop-up

Deveterumalistadenotificaçõesatuaiseanteriores

As notificações devem incluir: eventos AV, eventos ATP, eventos de comunicação, eventos de filtro da web e eventos do sistema.

Devefornecerinformaçõessobreavulnerabilidade,patches,versõesafetadasetc.,bemcomoo CVE correspondente

Devefornecerumalistadeaplicativosbloqueados

Casooclientefiqueemquarentena,devesercapazdeinformaraousuárioenotificaro gerenciamento.

Devesuportaraexibiçãodeumalistadeexploraçõesdetectadas.

Devepermitirexibirumalista deaplicativosprotegidoscontraexploração

Devefornecerumalistadearquivosemquarentena

DeveserpossívelvisualizarosresultadosdaanáliseATP.

ANÁLISEDEVULNERABILIDADE

Oclientedesegurançadeveterummódulodepesquisadevulnerabilidadesintegradoepermitir o gerenciamento central no console do mesmo fabricante

Devepermitirqueousuárioinicieumaanálisedevulnerabilidadesobdemanda

Asvulnerabilidadesencontradasdevemserexibidaslocalmentecomumlinkparavisualizar informações de um banco de dados na Internet. deve ter pelo menos: nome, gravidade e detalhes

Osresultadosdaverificaçãodevulnerabilidadesdeveincluirpelomenos:listade vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas.

Linksdeacessoainformaçõescomplementaresdevemserfornecidos,porexemplo,linksparaa página do fabricante onde as características da vulnerabilidade são detalhadas.

Devepermitiraaplicaçãoautomáticadepatches

Devedetalharquaiscorreçõesrequereminstalaçãomanual.

A verificação de vulnerabilidades deve ser permitida de maneira ordenada e autônoma a partir do console central

Deveverificarasvulnerabilidadesantesdeaplicarpatches

FUNCIONALIDADESDEFILTRODECONTEÚDOWEB

Deve permitir a configuração do perfil de filtro da web a partir do console central do mesmo fabricante

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

O cliente de segurança deve suportar regras estáticas de acesso à Internet com base em expressões regulares

ParaumdeterminadaURL,osacessosdevemser:permitir,bloquear,alertaroumonitorar

DeveconfigurarofiltrodeURLfornecidopelofabricantecompelomenosasseguintesações:

Bloquear,avisar,permitiremonitorar;

DeveconfigurarofiltrodeURLcombaseemcaracterescuringasouexpressõesregulares(regex) com as seguintes ações:

Bloquearoupermitir;

ITEM02–SOLUÇÃO PARA DUPLO FATOR DE AUTENTICAÇÃO-TOKEN MOBILE

Devepossuir05(cinco)licenciamentosperpétuosdetokenesemlimitesdetransferênciaparaoutros dispositivos.

Devepermitirodownloadgratuitonaslojasdeaplicativosseparadodoseuprovisionamento

Oaplicativodevesuportarexclusãoeadiçãodenovostokens

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

Devegarantiraprivacidadedodispositivomóvel,ouseja,nãodevesercapazdeconsultarhistóricode navegação

Deverequererapermissãoproprietárioparaenviodenotificaçõesouqualquertipodealteraçãonas configurações

Deve suportar as principais plataformas de mobile do mercado (iOS (iPhone, iPod Touch, iPad), Android, Windows Phone 8, 8.1, Windows 10)

Devesuportarageração dinâmicadassementesdetoken,minimizandoaexposiçãoonline.

DevesuportarativaçãoatravésdautilizaçãodeQRCodesemanual

Devecriptografaroarmazenamentodesementesutilizadasnageraçãodotoken

Devesercapazdegerarsenhasdeusoúnico(OneTimeProgrammable-OTP)baseadoemtempo(TOTP)ou evento (HTOP) compatível com OATH

Devesuportaraocultaçãodotokenparatokensbaseadosemtempo(TOTP)

DevecapazdeprotegeraberturadoaplicativoatravésdePINouImpressãoDigitalouFaceSecurity

Deveexibirointervalodetempo OTP

Deveexibirdonúmerodesériedotoken

DevesercompatívelcomorelógiodaApple

Devesuportarqueasenhageradapossasercopiadaparaaáreadetransferência

Devesuportardetalhesdeloginenviadosaotelefoneparaaprovaçãocomumtoque

Deveusarumserviçodeprovisionamentodinâmico,ondeapenasnaatribuiçãodeumtokenaumusuário a semente é criada e é removida durante o download ou após um tempo limite configurável.

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"

DeveestardeacordocomasseguintesRFCsparaespecificaçõesOTP:RFC6238eRFC4226

Devesercapazderealizarvinculaçãocomodispositivomóvel

Devesuportaràsuautilizaçãocomosegundofatorde autenticaçãoparaacessoVPNviaSSLouIPSEC, sem a necessidade de utilização de um servidor Radius

DevesercompatívelcomGoogle,Dropbox,AmazoneoutrostokensTOTP(Time-basedOne-Time Password) compatíveis com OAT.

ITEM03–SOLUÇAODESEGURANÇA DE REDE NGFWTIPOI

CARACTERISTICASGERAIS:

Soluçãobaseada emappliance.Para maior segurança,não serãoaceitosequipamentosdepropósito 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.

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.

Asoluçãodeveráserfornecidacomlicençasparautilizaçãoduranteavigênciacontratualde24(vinte e quatro)meses, com as funcionalidades habilitadas de Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro deConteúdoWeb, Antivírus, AntiSpam, Detecção ePrevenção deIntrusos(IPS),VPN IPSec e SSL, Controle de Aplicações.

Devepossuirfontedealimentaçãocomchaveamentoautomático110/220V.

Devepossuirfirewallcomcapacidademínimadeprocessamentode6(seis)Gbps.

DevepossuirIPScomcapacidademínimadeprocessamentode1(um)Gbps.

Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de600(seiscentos)Mbps,contemplandoasfunçõesdeFirewall,IPS,controledeaplicaçãoeproteção contra Malware/Antivírus ativadas de maneira simultâneas.

DevepossuirInspeçãoSSLThroughputcomcapacidademínimadeprocessamentode600(seiscentos) Mbps.

DevepossuirVPNcomcapacidadede,pelomenos,06(seis)GbpsdetráfegoIPSec.

Devesuportar600.000(seiscentosmil)conexõessimultâneas.

Deverãoserlicenciadosparasuportar,pelomenos,200(duzentos)usuáriosdeVPNSSL.

Devesuportar,pelomenos,30.000(trintamil)novasconexõesporsegundo.

Devesuportar,pelomenos,200(duzentos)túneisdeVPNSite-Site.

Devesuportar,pelomenos,200(duzentos)túneisdeVPNClient-Site.

Devepossuir,pelomenos,08(oito)interfacesRJ45.

DeveserfornecidaSoluçãodeGerênciaCentralizadadeEquipamentos,casocompatívelpoderá ser utilizada atual solução existente na PRODEB, Marca Fortinet, Modelo FMG-3000G.

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.

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

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

FUNCIONALIDADEDEFIREWALL

DevepossuircontroledeacessoàinternetporendereçoIPdeorigemedestino;

Devepossuircontroledeacessoàinternet porsubrede;

DevesuportartagsdeVLAN(802.1q);

Devepossuirferramentadediagnósticodotipotcpdump;

DevepossuirintegraçãocomservidoresdeautenticaçãoRADIUS,LDAPeMicrosoftActiveDirectory;

Devepossuirintegraçãocomtokensparaautenticaçãode02(dois)fatores;

Devesuportarsingle-sign-onparaActiveDirectory,RADIUS;

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

Devepossuirafuncionalidadedetraduçãodeendereçosestáticos–NAT(NetworkAddressTranslation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

Devepermitircontroledeacessoàinternetporperíodosdodia,permitindoaaplicaçãode políticas por horários e por dia da semana;

Devepermitircontroledeacessoàinternetpordomínio,porexemplo:gov.br,org.br,edu.br;

Devepossuirafuncionalidadedefazertraduçãodeendereçosdinâmicos,muitosparaum,PAT;

DevesuportarroteamentoestáticoedinâmicoRIPV1,V2,OSPF,ISISeBGPv4;

DevepossuirfuncionalidadesdeDHCPCliente,ServidoreRelay;

Devesuportaraplicaçõesmultimídia,como:H.323eSIP;

DevepossuirtecnologiadefirewalldotipoStatefull;

Devesuportaraltadisponibilidade(HA),trabalhandono esquemaderedundânciadotipoAtivo- Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

Deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;

DevesuportarPBR–PolicyBasedRouting;

DevepermitiracriaçãodeVLANSnopadrãoIEEE802.1q;

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

Deve permitirfiltrodepacotessem controledeestado(stateless)paraverificaçãoemcamada2;

Devepermitirforwardingdecamada2paraprotocolosnãoIP;

Devesuportarforwardingmulticast;

DevesuportarroteamentomulticastPIMSparseModeeDenseMode;

Devepermitircriaçãodeserviçosporportaouconjuntodeportasdosseguintesprotocolos:TCP, UDP, ICMP e IP;

Devepermitiroagrupamentodeserviços;

Devepermitirofiltrodepacotessemautilizaçãodenat;

Devepermitiraaberturadenovasportasporfluxodedadosparaserviçosquerequeremportas dinâmicas;

Devepossuirmecanismodeanti-spoofing;

Devepermitircriaçãoderegrasdefinidaspelousuário;

Devepermitiroserviçodeautenticaçãoparatráfegohttpe FTP;

DevepermitirIP/MACbinding,permitindoquecadaendereçoIPpossaserassociadoaum endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

Devepossuirafuncionalidadedebalanceamentoecontingênciadelinks;

DevesuportarsFlow;

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

Deveteracapacidadedecriareaplicarpolíticasdereputaçãodeclientepararegistrarepontuar 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;

Devepermitirautenticaçãodeusuáriosembaselocal,servidorLDAP,RADIUSeTACACS;

Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

DevesuportarcertificadosX.509,SCEP,CertificateSigningRequest(CSR)eOCSP;

Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN- tagged;

Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicaçõesdcerpc,dns-tcp,dns-udp,ftp,H.245I,H.2450,H.323,MGCP,MMS,PMAP,PPTP,RAS,RSH, SIP, TFTP, TNS;

DevesuportarSIP,H.323eSCCPNATTraversal;

Devepermitiracriaçãodeobjetoseagrupamentodeobjetosdeusuários,redes,FQDN, protocolos e serviços para facilitar a criação de regras;

Deve possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

FUNCIONALIDADEDETRAFFICSHAPINGEPRIORIZAÇÃODETRÁFEGO

Devepermitirocontroleeapriorizaçãodotráfego,priorizandoegarantindobandaparaasaplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

DevepermitirmodificaçãodevaloresDSCPparaoDiffServ;

DevepermitirpriorizaçãodetráfegoesuportarToS;

Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

Deveintegrar-seaoserviçodediretóriopadrãoLDAP,inclusiveoMicrosoftActiveDirectory, reconhecendo grupos de usuários cadastrados;

Deveproverfuncionalidadedeidentificaçãotransparentedeusuárioscadastradosnomicrosoft Active Directory e LDAP;

Devecontrolar(limitarouexpandir)individualmenteabandautilizadaporgrupodeusuáriosdo Microsoft Active Directory e LDAP;

Devepermitirdefinirbandamáximaebandagarantidaparaumusuário,IP,grupodeIPs,protocoloe aplicação;

Devecontrolar(limitarouexpandir)individualmenteabandautilizadaporsubrededeorigeme destino;

Devecontrolar(limitarouexpandir)individualmenteabandautilizadaporendereçoIPdeorigem e destino;

FUNCIONALIDADEDEANTI-SPAMDEGATEWAY

Devepermitir,nafuncionalidadedeanti-spam,verificaçãodocabeçalhoSMTPdotipoMIME;

Devepossuirfiltragemdee-mailporpalavraschaves;

Devepermitiradicionarrótuloaoassuntodamensagemquandoclassificadocomo SPAM;

Devepossuir,paraafuncionalidadedeanti-spam,orecursodeRBL;

Devepermitirachecagemdereputaçãodaurlnocorpomensagemdecorreioeletrônico;

FUNCIONALIDADEDEFILTRODECONTEÚDOWEB

Devepossuirsoluçãodefiltrodeconteúdowebintegradoàsoluçãodesegurança;

Devepossuir,pelomenos,70(setenta)categoriasparaclassificaçãodesitesweb;

Devepossuirbase mínima contendo100.000.000(cem milhões)de sitesinternet Web já registrados e classificados;

Devepossuirafuncionalidadedecotadetempodeutilizaçãoporcategoria;

Devepossuircategoriaexclusiva,nomínimo,paraosseguintestiposdesitesweb,como:

Proxyanônimo;

Webmail;

Instituiçõesdesaúde;

Notícias;

Phishing;

Hackers;

Pornografia;

Racismo;

Websitespessoais;

Compras;

Devepermitiramonitoraçãodotráfegointernetsembloqueiodeacessoaosusuários;

Devepermitiracriaçãode,pelomenos,07(sete)categoriaspersonalizadas;

DevepermitirareclassificaçãodesitesWeb,tantoporURL,quantoporendereço IP;

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;

Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory,reconhecendo contas e grupos de usuários cadastrados;

Deveproverfuncionalidadedeidentificaçãotransparentedeusuárioscadastradosno Microsoft Active Directory;

Devepossuirintegraçãocomtokensparaautenticaçãode02(dois)fatores;

Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

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;

Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

DevepermitirobloqueiodeURLsinválidas, cujo campo CN docertificadoSSLnão contenha um domínio válido;

Devefiltraroconteúdobaseadoemcategoriasemtemporeal;

Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

Devepermitiracriaçãoderegrasparaacesso/bloqueioporendereçoIPdeorigem;

Devepermitiracriaçãoderegrasparaacesso/bloqueioporsubredededeorigem;

DevesercapazdecategorizarapáginaWeb,tantopelasuaURL,comopeloseuendereçoIP;

Devepermitirobloqueioderedirecionamentohttp;

Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

DevepossuirProxyExplícitoeTransparente;

DeveimplementarroteamentoWCCPeICAP;

FUNCIONALIDADEDEDETECÇÃODEINTRUSÃO

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;

Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaçasconhecidas;

Deveestarorientadoàproteçãoderedes;

Devepermitirfuncionaremmodotransparente,sniffererouter;

Devepossuirtecnologiadedetecçãobaseadaemassinaturasquesejamatualizadas automaticamente;

Devepermitiracriaçãodepadrõesdeataquemanualmente;

Devepossuirintegraçãoàplataformadesegurança;

Devepossuircapacidadederemontagemdepacotesparaidentificaçãodeataques;

Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupartodasasassinaturasrelacionadasaweb-server,paraquesejausadoparaproteçãoespecífica de Servidores Web;

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;

Devepossuirmecanismosdedetecção/proteçãodeataques;

Devepossuirreconhecimentodepadrões;

Devepossuiranálisedeprotocolos;

Devepossuirdetecçãodeanomalias;

DevepossuirdetecçãodeataquesdeRPC(RemoteProcedureCall);

Devepossuirproteçãocontra-ataquesdeWindowsouNetBios;

Devepossuirproteçãocontra-ataquesdeSMTP(SimpleMessageTransferProtocol),IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

Devepossuirproteçãocontra-ataquesDNS(DomainNameSystem);

Devepossuirproteçãocontra-ataquesaFTP,SSH,TelneterIogin;

Devepossuirproteçãocontra-ataquesdeICMP(InternetControlMessageProtocol);

Devepossuirmétodosdenotificaçãodedetecçãodeataques;

Devepossuiralarmesnaconsolede administração;

Devepossuiralertasviacorreioeletrônico;

Devepossuirmonitoraçãodocomportamentodoappliance,medianteSNMP.Odispositivodeve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

Deveteracapacidadederesposta/logsativaaataques;

Deveproveraterminaçãodesessõesviatcpresets;

Devearmazenaroslogsdesessões;

Deveatualizarautomaticamenteasassinaturasparaosistemadedetecçãodeintrusos;

Devemitigarosefeitosdosataquesdenegaçãode serviços;

Devepermitiracriaçãodeassinaturaspersonalizadas;

Devepossuirfiltrosdeataquesporanomalias;

Devepermitirfiltrosdeanomaliasdetráfegoestatísticode: flooding, scan, sourceedestination session limit;

Devepermitirfiltrosdeanomaliasdeprotocolos;

Devesuportarreconhecimentodeataquesde DoS,reconnaissance,exploitseevasion;

Devesuportarverificaçãodeataquenacamadadeaplicação;

Devesuportarverificaçãodetráfegoemtemporeal,viaaceleraçãodehardware;

Devepossuirasseguintesestratégiasdebloqueio:pass,dropereset.

FUNCIONALIDADEDEVPN

Devepossuiralgoritmosdecriptografiaparatúneis VPN:AES,DES,3DES;

Devepossuirsuporteacertificados PKIX.509paraconstruçãodeVPNs;

DevepossuirsuporteaVPNsIPSeCSite-to-SiteeVPNsIPSecClient-to-Site;

DevepossuirsuporteaVPN SSL;

Devepossuircapacidadederealizar SSLVPNsutilizandocertificadosdigitais;

Devepossuirhardwareaceleradorcriptográficoparaincrementarodesempenhoda VPN;

AVPNSSLdevesuportarclienteparaplataformaWindows,LinuxeMacOSX;

DevepermitiraarquiteturadeVPNhubandspoke;

Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

FUNCIONALIDADEDECONTROLEDEAPLICAÇÕES

Devereconhecer,nomínimo,2.000(duasmil)aplicações;

Devepossuir,pelomenos,10(dez)categoriasparaclassificaçãodeaplicações;

Devepossuircategoriaexclusiva,nomínimo,paraosseguintestiposdeaplicações,como:

P2P

InstantMessaging;

Webclient;

Transferênciadearquivos;

VoIP;

Devepermitiramonitoraçãodotráfegodeaplicaçõesembloqueiodeacessoaosusuários;

Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando- as apenas pelo comportamento de tráfego da mesma;

Deveintegrar-seaoserviçodediretóriopadrãoLDAP,inclusiveoMicrosoftActiveDirectory, reconhecendo grupos de usuários cadastrados;

Deveproverfuncionalidadedeidentificaçãotransparentedeusuários cadastradosnoMicrosoft Active Directory;

Devepermitiracriaçãoderegrasparaacesso/bloqueiodeaplicaçõesporgrupodeusuáriosdo Microsoft Active Directory;

Devepermitiracriaçãoderegrasparaacesso/bloqueiodeaplicaçõesporgrupodeusuáriosdoserviço de diretório LDAP;

Devepermitiracriaçãoderegrasparaacesso/bloqueioporendereçoIPdeorigem;

Devepossuirintegraçãocomtokensparaautenticaçãode02(dois)fatores;

Devepermitiracriaçãoderegrasparaacesso/bloqueioporsubredededeorigemedestino;

Devepermitirainspeção/bloqueiodecódigosmaliciosospara,nomínimo,asseguintes categorias: Instant Messaging e transferência de arquivos;

Devegarantirqueasatualizaçõesregularesdoprodutosejamrealizadasseminterrompera execução dos serviços de controle de aplicações;

Devepermitircriaçãodepadrõesdeaplicaçãomanualmente;

FUNCIONALIDADEDEBALANCEAMENTODECARGA

Devepermitiracriaçãodeendereços IPsvirtuais;

Devesuportarbalanceamento,aomenos,paraosseguintesserviços:HTTP,HTTPS,TCPeUDP;

Devepermitirbalanceamento,aomenos,comosseguintesmétodos:HashdoendereçoIPdeorigem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;

DevepermitirpersistênciadesessãoporcookieHTTPouSSLsessionID;

Devepermitirquesejamantidoo**IP**deorigem;

DevesuportarSSLoffloadingnosequipamentosquesuportem,pelomenos,200(duzentos)usuários;

Deveteracapacidadededentificar,através**d**ehealthchecks,quaisosservidoresqueestejamativos, removendo automaticamente o tráfego dos servidores que não estejam;

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

FUNC**I**ONAL**I**DADEDESD-WAN

AsoluçãoSD-WANdeveserviabilizadacomrecursosdesegurançaintegradosde:Firewall,VPN, Antivírus, **I**PS e Fi**l**tro de Segurança Web.

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

AsoluçãoSD-WANdevesuportarsegmentaçãodetráfegoondesejapossívelaplicarpolíticasde **I**PS e Antivírus entre segmentos de LAN.

AsoluçãoSD-WANdeveprovercapacidadedeinspeçãoSSLparaainspeçãodetráfegohttpsnas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

SoluçãodevesercapazdeproverZeroTouchprovisioning.

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

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.

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

AconfiguraçãoVPN**I**PSECdeveoferecersuporteparaDHGroup:14e 15.

Reconhecimentoemcamada7totalmentesegregadodacamada4.

Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado **I**P/ range de **I**Ps de destino.

O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o pay**l**oad de pacote de dados;

AindasobreoreconhecimentodeAplicações,asoluçãodeveforneceroreconhecimentodefault 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)

AsoluçãodeSD-WANdevesuportarRoteamentodinâmicoBGPcomsuporteaI**P**v6

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.

A solução deveser capaz demedir o StatusdeSaúdedo Link baseando-seemcritériosmínimos 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.

A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenasocorreráquandoolinkprincipalrecuperadosejaX% (comXvariandode10à50)doseuvalor de saúde melhor que o link atual.

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.

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

ITEM04–SOLUÇAODESEGURANÇADEREDENGFWT**I**PO II

CARACTER**I**ST**I**CASGERA**I**S:

Asoluçãodeveser entregueno formatodesoluçãovirtual,compatívelcomasplataformasVMware, MicrosoftHyper-V,CitrixXenServer,OpenSourceXen,KVM,aresponsabilidadepelofornecimentoe a implantação de servidor/hardware com licenciamento necessário será da CONTRATADA, e o equipamento deve ser instalado no local indicado pela CONTRATANTE.

Asoluçãodeveráserfornecidacomlicençasparautilizaçãoduranteavigênciacontratualde24(vinte e quatro)meses, com as funcionalidades habilitadas de Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro deConteúdoWeb, Antivírus, AntiSpam, Detecção ePrevenção de**I**ntrusos(**I**PS),VPN **I**PSec e SSL, Controle de Aplicações.

Devesuportarepossuirlicenciamentoparaaté04 vCPU.

Devesuportarepossuirlicenciamentoparanominimo02GBdeMemória.

Devesuportarepossuirlicenciamentoparaaté10interfacesderede.

Devepossuirfirewallcomcapacidademínimadeprocessamentode2(dois)Gbps.

Devepossuir**I**PScomcapacidademínimadeprocessamentode3(três)Gbps.

Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1,7 (um virgula sete) Gbps, contemplando as funções de Firewall, **I**PS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

DevepossuirVPNcomcapacidadede,pelomenos,2(dois)GbpsdetráfegoI**P**Sec.

Devesuportar5.000.000(cincomilhões)conexõessimultâneas.

Devesuportar,pelomenos,100.000(cemmil)novasconexõesporsegundo.

DeveserfornecidaSoluçãodeGerênciaCentralizadadeEquipamentos,casocompatívelpoderá ser utilizada atual solução existente na PRODEB, Marca Fortinet, Modelo FMG-3000G.

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.

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

Deveserfornecidatodadocumentaçãotécnicaemformatodigital,através**d**eacessoaURL oficial do fabricante, em português do Brasil ou em inglês.

FUNC**I**ONAL**I**DADEDE**F**IREWALL

Devepossuircontroledeacessoàinternetporendereço**I**Pdeorigemedestino;

Devepossuircontroledeacessoàinternetporsub rede;

DevesuportartagsdeVLAN(802.1q);

Devepossuirferramentadediagnósticodotipotcpdump;

Devepossuirintegraçãocomservidoresdeautenticação**R**AD**I**US,LDAPeMicrosoftActiveDirectory;

Devepossuirintegraçãocomtokensparaautenticaçãode02(dois)fatores;

Devesuportarsingle-sign-onparaActiveDirectory,RAD**I**US;

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

Devepossuirafuncionalidadedetraduçãodeendereçosestáticos–NAT(NetworkAddressTranslation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

Devepermitircontroledeacessoàinternetporperíodosdodia,permitindoaaplicaçãode políticas por horários e por dia da semana;

Devepermitircontroledeacessoàinternetpordomínio,porexemplo:gov.br,org.br,edu.br;

Devepossuirafuncionalidadedefazertraduçãodeendereçosdinâmicos,muitosparaum,PAT;

Devesuportarroteamentoestáticoedinâmico RIPV1,V2,OSPF,ISISeBGPv4;

DevepossuirfuncionalidadesdeDHCPCliente,ServidoreRelay;

Devesuportaraplicaçõesmultimídia,como:H.323eSIP;

Devepossuirtecnologiadefirewalldotipo Statefull;

Devesuportaraltadisponibilidade(HA),trabalhandonoesquemaderedundânciadotipoAtivo- Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

Deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;

DevesuportarPBR–PolicyBasedRouting;

DevepermitiracriaçãodeVLANSnopadrãoIEEE802.1q;

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

Deve permitirfiltrodepacotessemcontroledeestado(stateless)paraverificaçãoemcamada2;

Devepermitirforwardingdecamada2paraprotocolosnãoIP;

Devesuportarforwardingmulticast;

DevesuportarroteamentomulticastPIMSparseModeeDenseMode;

Devepermitircriaçãodeserviçosporportaouconjuntodeportasdosseguintesprotocolos:TCP, UDP, ICMP e IP;

Devepermitiroagrupamentodeserviços;

Devepermitirofiltrodepacotessemautilizaçãode NAT;

Devepermitiraaberturadenovasportasporfluxodedadosparaserviçosquerequeremportas dinâmicas;

Devepossuirmecanismodeanti-spoofing;

Devepermitircriaçãoderegrasdefinidaspelousuário;

Devepermitiroserviçodeautenticaçãoparatráfego HTTPe FTP;

DevepermitirIP/MACbinding,permitindoquecadaendereçoIPpossaserassociadoaum endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

Devepossuirafuncionalidadedebalanceamentoecontingênciadelinks;

DevesuportarsFlow;

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

Deveteracapacidadedecriareaplicarpolíticasdereputaçãodeclientepararegistrarepontuar 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;

Devepermitirautenticaçãodeusuáriosembaselocal,servidorLDAP,RADIUSeTACACS;

Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

DevesuportarcertificadosX.509,SCEP,CertificateSigningRequest(CSR)eOCSP;

Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN- tagged;

Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicaçõesdcerpc,dns-tcp,dns-udp,ftp,H.245I,H.2450,H.323,MGCP,MMS,PMAP,PPTP,RAS,RSH, SIP, TFTP, TNS;

DevesuportarSIP,H.323eSCCPNATTraversal;

Devepermitiracriaçãodeobjetoseagrupamentodeobjetosdeusuários,redes,FQDN, protocolos e serviços para facilitar a criação de regras;

Deve possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

FUNCIONALIDADEDETRAFFICSHAPINGEPRIORIZAÇÃODETRÁFEGO

Devepermitirocontroleeapriorizaçãodotráfego,priorizandoegarantindobandaparaasaplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

DevepermitirmodificaçãodevaloresDSCPparaoDiffServ;

DevepermitirpriorizaçãodetráfegoesuportarToS;

Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

Deveintegrar-seaoserviçodediretóriopadrãoLDAP,inclusiveoMicrosoftActiveDirectory, reconhecendo grupos de usuários cadastrados;

Deveproverfuncionalidadedeidentificaçãotransparentedeusuárioscadastradosno Microsoft Active Directory e LDAP;

Devecontrolar(limitarouexpandir)individualmenteabandautilizadaporgrupodeusuáriosdo Microsoft Active Directory e LDAP;

Devepermitirdefinirbandamáximaebandagarantidaparaumusuário,IP,grupodeIPs,protocoloe aplicação;

Devecontrolar(limitarouexpandir)individualmenteabandautilizadaporsubrededeorigeme destino;

Devecontrolar(limitarouexpandir)individualmenteabandautilizadaporendereçoIPdeorigem e destino;

FUNCIONALIDADEDEANTI-SPAMDEGATEWAY

Devepermitir,nafuncionalidadedeanti-spam,verificaçãodocabeçalhoSMTPdotipoMIME;

Devepossuirfiltragemdee-mailporpalavraschaves;

Devepermitiradicionarrótuloaoassuntodamensagemquandoclassificadocomo SPAM;

Devepossuir,paraafuncionalidadedeanti-spam,orecursodeRBL;

DevepermitirachecagemdereputaçãodaURLnocorpomensagem decorreioeletrônico;

FUNCIONALIDADEDEFILTRODECONTEÚDOWEB

Devepossuirsoluçãodefiltrodeconteúdo Webintegradoàsoluçãodesegurança;

Devepossuir,pelomenos,70(setenta)categoriasparaclassificaçãodesitesWeb;

Devepossuirbase mínima contendo100.000.000(cem milhões)de sitesinternet Web já registrados e classificados;

Devepossuirafuncionalidadedecotadetempodeutilizaçãoporcategoria;

Devepossuircategoriaexclusiva,nomínimo,paraosseguintestiposdesitesWeb,como:

Proxyanônimo;

Webmail;

Instituiçõesdesaúde;

Notícias;

Phishing;

Hackers;

Pornografia;

Racismo;

Websitespessoais;

Compras;

Devepermitiramonitoraçãodotráfegointernetsembloqueiodeacessoaosusuários;

Devepermitiracriaçãode,pelomenos,07(sete)categoriaspersonalizadas;

DevepermitirareclassificaçãodesitesWeb,tantoporURL,quantoporendereço IP;

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;

Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory,reconhecendo contas e grupos de usuários cadastrados;

Deveproverfuncionalidadedeidentificaçãotransparentedeusuárioscadastradosno Microsoft Active Directory;

Devepossuirintegraçãocomtokensparaautenticaçãode02(dois)fatores;

Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

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;

Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

DevepermitirobloqueiodeURLsinválidas, cujo campo CN docertificadoSSLnão contenha um domínio válido;

Devefiltraroconteúdobaseadoemcategoriasemtemporeal;

Devegarantirqueasatualizaçõesregularesdoprodutosejamrealizadasseminterrompera execução dos serviços de filtragem de conteúdo Web;

Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço dediretório LDAP;

DevepermitiracriaçãoderegrasparaacessoIP/bloqueioporendereçoIPdeorigem;

DevepermitiracriaçãoderegrasparaacessoIP/bloqueioporsubredededeorigem;

DevesercapazdecategorizarapáginaWeb,tantopelasuaURL,comopeloseuendereçoIP;

DevepermitirobloqueioderedirecionamentoHTTP;

Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

DevepossuirProxyExplícitoeTransparente;

DeveimplementarroteamentoWCCPeICAP;

FUNCIONALIDADEDEDETECÇÃODEINTRUSÃO

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;

Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaçasconhecidas;

Deveestarorientadoàproteçãoderedes;

Devepermitirfuncionaremmodotransparente,sniffererouter;

Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

Devepermitiracriaçãodepadrõesdeataquemanualmente;

Devepossuirintegraçãoàplataformadesegurança;

Devepossuircapacidadederemontagemdepacotesparaidentificaçãodeataques;

Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupartodasasassinaturasrelacionadasaweb-server,paraquesejausadoparaproteçãoespecífica de Servidores Web;

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;

Devepossuirmecanismosdedetecção/proteçãodeataques;

Devepossuirreconhecimentodepadrões;

Devepossuiranálisedeprotocolos;

Devepossuirdetecçãodeanomalias;

DevepossuirdetecçãodeataquesdeRPC(RemoteProcedureCall);

DevepossuirproteçãocontraataquesdeWindowsouNetBios;

Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

DevepossuirproteçãocontraataquesDNS(DomainNameSystem);

DevepossuirproteçãocontraataquesaFTP,SSH,Telneterlogin;

Devepossuirproteçãocontra-ataquesdeICMP(InternetControlMessageProtocol);

Devepossuirmétodosdenotificaçãodedetecçãodeataques;

Devepossuiralarmesnaconsoledeadministração;

Devepossuiralertasviacorreioeletrônico;

Devepossuirmonitoraçãodocomportamentodoappliance,medianteSNMP.Odispositivodeve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

Deveteracapacidadederesposta/logsativaaataques;

Deveproveraterminaçãodesessõesviatcpresets;

Devearmazenaroslogsdesessões;

Deveatualizarautomaticamenteasassinaturasparaosistemadedetecçãodeintrusos;

Devemitigarosefeitosdosataquesdenegaçãodeserviços;

Devepermitiracriaçãodeassinaturaspersonalizadas;

Devepossuirfiltrosdeataquesporanomalias;

Devepermitirfiltrosdeanomaliasdetráfegoestatísticode: flooding, scan, sourceedestination session limit;

Devepermitirfiltrosdeanomaliasdeprotocolos;

Devesuportarreconhecimentodeataquesdedos,reconnaissance,exploitseevasion;

Devesuportarverificaçãodeataquenacamadadeaplicação;

Devesuportarverificaçãodetráfegoemtemporeal,viaaceleraçãodehardware;

Devepossuirasseguintesestratégiasdebloqueio:pass,dropereset.

FUNCIONALIDADEDEVPN

Devepossuiralgoritmosdecriptografiaparatúneisvpn:aes,des,3des;

DevepossuirsuporteacertificadospkIX.509paraconstruçãodevpns;

DevepossuirsuporteaVPNsIPSeCSite-to-SiteeVPNsIPSecClient-to-Site;

DevepossuirsuporteaVPN SSL;

DevepossuircapacidadederealizarSSLVPNsutilizandocertificadosdigitais;

Devepossuirhardwareaceleradorcriptográficoparaincrementarodesempenhodavpn;

AVPNSSLdevesuportarclienteparaplataformaWindows,LinuxeMacOSX;

DevepermitiraarquiteturadeVPNhubandspoke;

Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

FUNCIONALIDADEDECONTROLEDEAPLICAÇÕES

Devereconhecer,nomínimo,2.000(duasmil)aplicações;

Devepossuir,pelomenos,10(dez)categoriasparaclassificaçãodeaplicações;

Devepossuircategoriaexclusiva,nomínimo,paraosseguintestiposdeaplicações,como:

P2P

InstantMessaging;

Webclient;

Transferênciadearquivos;

VoIP;

Devepermitiramonitoraçãodotráfegodeaplicaçõesembloqueiodeacessoaosusuários;

Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando- as apenas pelo comportamento de tráfego da mesma;

Deveintegrar-seaoserviçodediretóriopadrãoLDAP,inclusiveoMicrosoftActiveDirectory, reconhecendo grupos de usuários cadastrados;

Deveproverfuncionalidadedeidentificaçãotransparentedeusuárioscadastradosnomicrosoft Active Directory;

Devepermitiracriaçãoderegrasparaacesso/bloqueiodeaplicaçõesporgrupodeusuáriosdo Microsoft Active Directory;

Devepermitiracriaçãoderegrasparaacesso/bloqueiodeaplicaçõesporgrupodeusuáriosdoserviço de diretório LDAP;

Devepermitiracriaçãoderegrasparaacesso/bloqueioporendereçoIPdeorigem;

Devepossuirintegraçãocomtokensparaautenticaçãode02(dois)fatores;

Devepermitiracriaçãoderegrasparaacesso/bloqueioporsubredededeorigemedestino;

Devepermitirainspeção/bloqueiodecódigosmaliciosospara,nomínimo,asseguintes categorias: Instant Messaging e transferência de arquivos;

Devegarantirqueasatualizaçõesregularesdoprodutosejamrealizadasseminterrompera execução dos serviços de controle de aplicações;

Devepermitircriaçãodepadrõesdeaplicaçãomanualmente;

FUNCIONALIDADEDEBALANCEAMENTODECARGA

DevepermitiracriaçãodeendereçosIPsvirtuais;

Devesuportarbalanceamento,aomenos,paraosseguintesserviços:HTTP,HTTPS,TCPeUDP;

Devepermitirbalanceamento,aomenos,comosseguintesmétodos:HashdoendereçoIPdeorigem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;

DevepermitirpersistênciadesessãoporcookieHTTPouSSLsessionID;

DevepermitirquesejamantidooIPdeorigem;

DevesuportarSSLoffloadingnosequipamentosquesuportem,pelomenos,200(duzentos)usuários;

Deveteracapacidadedeidentificar,atravésdehealthchecks,quaisosservidoresqueestejamativos, removendo automaticamente o tráfego dos servidores que não estejam;

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

FUNCIONALIDADEDESD-WAN

AsoluçãoSD-WANdeveserviabilizadacomrecursosdesegurançaintegradosde:Firewall,VPN, Antivírus, IPS e Filtro de Segurança Web.

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

AsoluçãoSD-WANdevesuportarsegmentaçãodetráfegoondesejapossívelaplicarpolíticasde IPS e Antivírus entre segmentos de LAN.

AsoluçãoSD-WANdeveprovercapacidadedeinspeçãoSSLparaainspeçãodetráfegohttpsnas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

SoluçãodevesercapazdeproverZeroTouchprovisioning.

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

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.

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.

AconfiguraçãoVPNIPSECdeveoferecersuporteparaDH Group:14e 15.

Reconhecimentoemcamada7totalmentesegregadodacamada4.

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.

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

AindasobreoreconhecimentodeAplicações,asoluçãodeveforneceroreconhecimentodefault 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)

AsoluçãodeSD-WANdevesuportarRoteamentodinâmicoBGPcomsuporteaIPv6

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.

A solução deveser capaz demedir o StatusdeSaúdedo Link baseando-seemcritériosmínimos 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.

A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenasocorreráquandoolinkprincipalrecuperadosejaX% (comXvariandode10à50)doseuvalor de saúde melhor que o link atual.

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.

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

ITEM05–SOLUÇÃODESEGURANÇADEAPLICAÇÕESWAFTIPOI

CARACTERÍSTICASEFUNCIONALIDADESGERAIS

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 licenciamentonecessárioseráda CONTRATADA,eoequipamentodeveserinstaladonolocalindicado pela CONTRATANTE.

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

Asoluçãodeveráserfornecidacomlicençasparautilizaçãoduranteavigênciacontratualde24(vinte equatro)meses, comasfuncionalidadeshabilitadasdeAV, IPS,WAF SecurityService, IP Reputation, Sandbox, Credential Stuffing Defense Service.

RequisitosMínimosdePerformance

DevepossuirthroughputmínimoparaHTTPde450(quatrocentosecinquenta)Mbps;

Devesuportarquantidadeilimitadadeaplicaçõesprotegidas;

Devesuportaraté10interfacesderede;

Devesuportaraté04vCPU;

RequisitosMínimosdeFuncionalidades

Todososequipamentosquecompõemasoluçãodevemserentreguescomaúltimaversãode software homologada e recomendada pelo fabricante.

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.

Asolução proposta devecontemplar para a solução dearmazenamento, análisedelogse relatoria o projeto de implantação, migração, garantia, capacitação da equipe local e suporte.

FuncionalidadesdeRede

AsoluçãodevesercapazdeserimplementadanomodoProxy(TransparenteeReverso), Passivo,ou “Sniffer”

(Offline)eInlineTransparente(Bridge).

AsoluçãodevesercapazdeserimplementadacomprotocoloWCCP.

SuportarVLANsnopadrãoIEEE802.1q.

DeveimplementaroprotocolodenegociaçãoLinkAggregationControlProtocol(LACP)-IEEE 802.3ad.

SuportarendereçamentoIPv4eIPv6nasinterfacesfísicasevirtuais(VLANs).

Asoluçãodevesuportarroteamentoporpolítica(policyroute).

FuncionalidadesdeGerência

Osistemaoperacional/firmwaredevesuportarinterfacegráficawebparaaconfiguraçãodasfunções 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.

DevepossuiradministraçãobaseadaeminterfacewebHTTPS.

Possuirauto-complementaçãodecomandosnaCLI.

PossuirajudacontextualnaCLI.

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).

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

Deveprover,nainterfacede gerência,as seguintesinformaçõesdosistemaparacadagateway: consumo de CPU e estatísticas das conexões.

Deveserpossívelvisualizarnainterfacedegerênciaasinformaçõesdeconsumodememória.

DeveserpossívelvisualizarnainterfacedegerênciaouCLIasinformaçõesdeutilização odedisco de log.

Devepossuirferramenta,nainterfacegráficadegerência(dashboard)quepermita visualizaros últimos logs de ataque detectados/bloqueados.

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.

Possuirnainterfacegráficaestatísticasdeconexõesconcorrenteseporsegundo,depolíticasde segurança do sistema.

Possuirumpaineldevisualização comoinformações dasinterfacesderededosistema.

Aconfiguração deadministração dasolução devepossibilitarautilização deperfis.

Deveserpossívelexecutarerestaurarbackupviainterface Web(GUI).

Deveteraopção paracriptografarobackup.

Deveserpossívelexecutarerestaurarbackuputilizando-seumoumaisdosseguintesprotocolos: FTP, SFTP ou TFTP,ou HTTPS

Deveserpossívelinstalarumfirmwarealternativoemdiscoeinicializá-lomanualmenteemcaso de falha do firmware principal.

DevetersuporteaoprotocolodemonitoraçãoSNMPv1,SNMPv2ceSNMP v3.

Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog.

A solução deve ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG.

Teracapacidadedearmazenarlogsemappliance remoto.

A solução deve ter a capacidade de adicionar identificadores customizados nos registros syslog antes de envio, como hostname, atrelados a valores fixos ou variáveis.

A solução deve ter a capacidade de enviar alertas por e-mail de eventos baseados em severidades e/ou categorias.

Asolução devepossuirdadosanalíticoscontendolocalização geográficadosclientesweb.

Asolução devepossuirdadosanalíticos,sendopossívelvisualizaracontagemtotaldeataquese 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.

Deve ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário.

DevetersuporteaRESTfulAPIparagerenciamentodeconfigurações.

Devesuportartodasasfuncionalidadesparacomunicação HTTP/2

FuncionalidadesdeAutenticação

Osusuáriosdevemsercapazesdeautenticaratravésdocabeçalhodeautorização HTTP/HTTPS.

OsusuáriosdevemsercapazesdeautenticaratravésdeformuláriosHTMLembutidos.

Asolução devesercapazdeautenticarusuáriosatravésdecertificadosdigitaispessoais.

Devepossuirbaselocalparaarmazenamentoeautenticação contasdeusuários.

Asolução deveteracapacidadedeautenticarusuáriosembasesexternas/remotasLDAPeRADIUS.

OsusuáriosdevemsercapazesdeautenticaratravésdecontasdeusuáriosembaseremotaNTLM.

Asolução devesercapazdecriargruposdeusuáriosparaacessossemelhantesnaautenticação.

FuncionalidadesdeWebApplicationFirewall

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.

DeveimplementarrecursosdeSandboxparaanálisedemalwaremoderno;

Deveimplementarrecursodemachinelearning,ondeserápermitidoimplementarproteção paraum 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.

Deve implementar proteção contra a lista de técnicas/ataques listados no OWASP 10 (Open Web Application security Project)

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.

Teracapacidadedecriação deassinaturasdeataquecustomizáveis.

Teracapacidadedeproteção paraataquesdotipoAdobeFlashbinary(AMF)protocol.

Teracapacidadedeproteção paraataquesdotipoBotnet.

Teracapacidadedeproteção paraataquesdotipoBrowserExploitAgainstSSL/TLS(BEAST).

A solução deve possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta.

Devesuportardetecção aataquesdeClickjacking.

Devesuportardetecção aataquesdealteração decookie.

Deveidentificarepreveniratagues dotipoCreditCardTheft.

DeveidentificarepreveniratagueCrossSiteRequestForgery(CSRF).

Asolução devepossuirfuncionalidadedeproteção positivacontraataquescomocrosssite scripting (XSS).

DevepossuirproteçãocontraataquesdeDenialofService(DoS).

DevepossuiracapacidadedeproteçãoparaataquesdotipoHTTPheaderoverflow.

DevepossuiracapacidadedeproteçãoparaataquesdotipoLocalFileinclusion(FLI).

DevepossuiracapacidadedeproteçãoparaataquesdotipoMan-in-the-middle(MITM).

DevepossuiracapacidadedeproteçãoparaataquesdotipoRemoteFileInclusion(RFI).

DevepossuiracapacidadedeproteçãoparaataquesdotipoServerInformationLeakage.

Deve possuir proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection).

DevepossuiracapacidadedeproteçãoparaataquesdotipoMalformedXML.

DeveIdentificarepreveniratagues dotipoLow-rateDoS.

DevepossuirprevençãocontraSlowPOSTattack.

DeveprotegercontraataquesSlowloris.

DevepossuiracapacidadedeproteçãoparaataquesdotipoSYNflood.

DevepossuiracapacidadedeproteçãoparaataquesdotipoFormsTampering.

A solução deve possuir funcionalidade de proteção positiva contra ataques de manipulação de campo escondido.

DevepossuiracapacidadedeproteçãoparaataquesdotipoDirectoryTraversal.

DevepossuiracapacidadedeproteçãodotipoAccessRateControl.

DevepossuirahabilidadedeconfigurarproteçãodotipoTCPSYNflood-styleparaprevençãode DoS para qualquer política, através de Syn Cookie e Half Open Threshold.

DevepermitirconfigurarregrasdebloqueioamétodosHTTPindesejados.

DevepermitirquesejamconfiguradasregrasdelimitedeuploadportamanhodearquivO.

DevepermitirqueoadministradorbloqueieotráfegodeentradaE/outráfegodesaídacombase nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país.

Deve permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem.

Deve permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.

Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation.

Deve possuir a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP.

Devepossuirafuncionalidadedeprotegerowebsitecontraaçõesdedesfiguração(defacement), com restauração automática e rápida do site caso ocorra à falha.

DevepossuirafuncionalidadedeantivírusparainspeçãodetráfegoearquivOs.

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.

DevesercapazdefazeraceleraçãodeSSL,ondeoscertificadosdigitaissãoinstaladosnasolução e as requisições HTTP são enviadas aos servidores sem criptografia.

A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego.

DeveparaSSL/TLSoffloadsuportarnomínimoTLS1.0,1.1,1.2e1.3.

AsoluçãodeveteracapacidadedearmazenarcertificadosdigitaisdeCA's.

AsoluçãodevesercapazdegerarCSRparaserassinadoporumaCA.

A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL).

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.

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.

Asoluçãodevesercapazdelimitarototaldeconexõespermitidasparacadaservidorrealdeum pool de servidores.

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.

Asolução devepermitir criar regrasdefinindoa ordem em queaspáginasdevem seracessadas para prevenir ataques como cross-site request forgery (CSRF).

AsoluçãodeveteracapacidadededefinirrestriçõesamétodosHTTP.

Asoluçãodeveteracapacidadedeprotegercontraadetecçãodecamposocultos.

Deve permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares.

A solução deve incluir capacidade de atuar como um scanner de vulnerabilidades ou permitir a integraçãocomscannersdevulnerabilidadedeterceirosparadiagnósticoeidentificaçãodeameaças nos servidores web, software desatualizado e potenciais buffers overflows,

DevegerarperfildeproteçãoautomaticamenteapartirderelatórioemformatoXMLgeradopor scanner de vulnerabilidade de terceiros.

AsoluçãodevegerarumrelatóriodaanálisedevulnerabilidadesnoformatoHTML.

AsoluçãodevepermitiraexclusãodeURLsnaanálisedevulnerabilidades.

DevesercapazdefazercompressãodeconteúdoHTTP,parareduziraquantidadede informações enviadas ao cliente.

DevesuportarredireçãoereescritaderequisiçõeserespostasHTTP.

DevepermitirredirecionarrequisiçõesHTTPparaHTTPS.

DevepermitirreescreveralinhaURLnocabeçalhodeumarequisiçãoHTTP.

DevepermitirreescreverocampO"Host:"nocabeçalhodeumarequisiçãoHTTP.

DevepermitirreescreverocampO"Referer:"nocabeçalhodeumarequisiçãoHTTP.

DevepermitirredirecionarrequisiçõesparaoutrowebsitE.

PermitirenviarrespostaHTTP403ForbiddenpararequisiçõesHTTP.

DevepermitirreescreveroparâmetrO"Location:"nocabeçalhoHTTPdeumarespostade redireção HTTP de um servidor web.

DevepermitirreescreverocorpO("body")deumarespostaHTTPdeumservidorweb.

DevepermitiradicionarocampoX-Forwarded-Forparaidentificaçãodoendereçorealdocliente quando no modo de proxy reverso.

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).

A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizandomecanismoscomoHTMLForm,BasiceSuporteaSSO,métodoscomoLDAPeRADIUSpara consultas e integração dos usuários da aplicação.

PossuircapacidadedecachingparaaceleraçãoweB.

Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.

DevesuportarnomínimO500regrasdereescritaURLdistintas

DevesuportarnomínimO250políticasdeassinaturadistintas

DevesuportarnomínimO500gruposoupoolsdeservidores,ecadapooldevesuportarno mínimo 1000 membros

Devesuportarnomínimo1000IPsvirtuaisconfiguradoseativossimultaneamente

Devesercapazderestringiracessoquandoasrequisiçõesnãotiveremumcabeçalho HTTP específico pré-configurado.

Devesercapazdelimitaronúmerodeusuários/origenssimultâneosacessandoamesma conta/sessão/login.

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.

DevesercapazdeadicionarmúltiplosservidoresADFSemumpooldeservidores

Deveimplementar recursosdeproteção deAPI (Application Programming Interface) atravésde Machine learning, implementando a análise dinâmica das chamadas de API para detecção de anomalias e bloqueando ataques direcionados a aplicações baseadas em microserviços.

Outrasfuncionalidades

Asoluçãodeveincluirfuncionalidadedebalanceamentodecargaentreservidoresweb.

Devepossuirahabilidadedeconfigurarportasnão-padrãoparaaplicaçãowebHTTPeHTTPS.

Devepossuiracapacidadedebalancear/distribuirtráfegoerotearoconteúdoatravésdevários servidores web.

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

DevesuportaralgoritmoRoundRobinparabalanceamentodecargadeservidores.

DevesuportaralgoritmoWeightedRoundRobinparabalanceamentodecargadeservidores.

DevesuportaralgoritmoLeastConnectionsparabalanceamentodecargadeservidores.

Asoluçãodevesercapazdecriarservidoresvirtuaisquedefinemainterfacederede/bridgee endereço IP por onde o tráfego destinado ao Server Pool é recebido.

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

DeveserpossívelespecificaronúmeromáximodeconexõesTCPsimultâneasparaumdeterminado servidor membro do Server Pool.

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoTCP.

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoICMPECHO_REQUEST (ping).

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoTCPHalfOpen.

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoTCPSSL.

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoHTTP.

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoHTTPS.

NostestesdedisponibilidadeHTTPeHTTPS,permitirindicaraURLexataasertestada.

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

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

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

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

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

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

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

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

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

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

doCertificadoX509”.

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

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

A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando parâmetros do header HTTP.

A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada.

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.

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).

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

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

Asolução sercapazdebalancearassessõesnovas,maspreservar sessõesexistentesnomesmo servidor, implementando persistência baseada em ASP Session ID.

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

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

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

Asoluçãodevesercapazdeenviarcódigodeerro503caso ohelth-checkdosservidoresestiver desabilitado e/ou o servidor/serviço de retaguarda não estiver responsivo.

DevesuportarFWMARK(marcaçãodetráfego).

ITEM 06–SOLUÇÃO DE SEGURANÇA DE APLICAÇÕES WAFTIPOII

CARACTERÍSTICASEFUNCIONALIDADESGERAIS

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 licenciamentonecessárioserádaCONTRATADA,eoequipamentodeveserinstaladonolocalindicado pela CONTRATANTE.

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

Asoluçãodeveráserfornecidacomlicençasparautilizaçãoduranteavigênciacontratualde24(vinte equatro)meses, comasfuncionalidadeshabilitadasdeAV, IPS,WAF SecurityService, IP Reputation, Sandbox, Credential Stuffing Defense Service.

RequisitosMínimosdePerformance

DevepossuirthroughputmínimoparaHTTPde6(seis) Gbps;

Devesuportarquantidadeilimitadadeaplicaçõesprotegidas;

Devesuportaraté10interfacesderede;

Devesuportaraté16vCPU;

RequisitosMínimosdeFuncionalidades

Todososequipamentosquecompõemasolucãodevemserentreguescomaúltimaversãode software homologada e recomendada pelo fabricante.

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.

Asolução proposta devecontemplar para a solução dearmazenamento, análisedelogse relatoria o projeto de implantação, migração, garantia, capacitação da equipe local e suporte.

FuncionalidadesdeRede

AsoluçãodevesercapazdeserimplementadanomodoProxy(TransparenteeReverso), Passivo,ou “Sniffer”

(Offline)eInlineTransparente(Bridge).

AsoluçãodevesercapazdeserimplementadacomprotocoloWCCP.

SuportarVLANsnopadrãoIEEE802.1q.

DeveimplementaroprotocolodenegociaçãoLinkAggregationControlProtocol(LACP)-IEEE 802.3ad.

SuportarendereçamentoIPv4eIPv6nasinterfacesfísicasevirtuais(VLANs).

Asoluçãodevesuportarroteamentoporpolítica(policyroute).

FuncionalidadesdeGerência

Osistemaoperacional/firmwaredevesuportarinterfacegráficawebparaaconfiguraçãodasfunções 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.

DevepossuiradministraçãobaseadaeminterfacewebHTTPS.

Possuirauto-complementaçãodecomandosnaCLI.

PossuirajudacontextualnaCLI.

AsoluçãodevepossuirInterfaceGráficacominformaçõessobreosistemaEx:(Informaçõesdo Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware).

Deveserpossívelvisualizaratravésdainterfacegráficadegerênciainformaçõesdelicençase assinaturas.

Deveprover,nainterfacedegerência,asseguintesinformaçõesdosistemaparacadagateway: consumo de CPU e estatísticas das conexões.

Deveserpossívelvisualizarnainterfacedegerênciaasinformaçõesdeconsumodememória.

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

Devepossuir ferramenta,nainterfacegráficadegerência(dashboard)quepermita visualizaros últimos logs de ataque detectados/bloqueados.

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.

Possuirnainterfacegráficaestatísticasdeconexõesconcorrenteseporsegundo,depolíticasde segurança do sistema.

Possuirumpaineldevisualizaçãocominformaçõesdasinterfacesderededosistema.

Aconfiguraçãodeadministraçãodasoluçãodevepossibilitarautilizaçãodeperfis.

Deveserpossívelexecutarerestaurarbackupviainterface Web(GUI).

Deveteraopçãoparacriptografarobackup.

Deveserpossívelexecutarerestaurarbackuputilizando-seumoumaisdosseguintesprotocolos: FTP, SFTP ou TFTP,ou HTTPS

Deveserpossívelinstalarumfirmwarealternativoemdiscoeinicializá-lomanualmenteemcaso de falha do firmware principal.

Devetersuporteaoprotocolodemonitoraçãoo SNMPv1,SNMPv2ceSNMP v3.

Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog.

A solução deve ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG.

Teracapacidadedearmazenarlogsemappliance remoto.

A solução deve ter a capacidade de adicionar identificadores customizados nos registros syslog antes de envio, como hostname, atrelados a valores fixos ou variáveis.

A solução deve ter a capacidade de enviar alertas por e-mail de eventos baseados em severidades e/ou categorias.

Asoluçãodevepossuirdadosanalíticoscontendolocalizaçãogeográficadosclientesweb.

Asoluçãodevepossuirdadosanalíticos,sendopossívelvisualizaracontagemtotaldeataquese 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.

Deve ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário.

DevetersuporteaRESTfulAPIparagerenciamentodeconfigurações.

DevesuportartodasasfuncionalidadesparacomunicaçãoHTTP/2

FuncionalidadesdeAutenticação

OsusuáriosdevemsercapazesdeautenticaratravésdocabeçalhodeautorizaçãoHTTP/HTTPS.

OsusuáriosdevemsercapazesdeautenticaratravésdeformuláriosHTMLembutidos.

Asoluçãodevesercapazdeautenticarusuáriosatravésdecertificadosdigitaispessoais.

Devepossuirbaselocalparaarmazenamentoeautenticaçãocontasdeusuários.

Asoluçãodeveteracapacidadedeautenticarusuáriosembasesexternas/remotasLDAPeRADIUS.

OsusuáriosdevemsercapazesdeautenticaratravésdecontasdeusuáriosembaseremotaNTLM.

Asoluçãodevesercapazdecriargruposdeusuáriosparaacessossemelhantesnaautenticação.

FuncionalidadesdeWebApplicationFirewall

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.

DeveimplementarrecursosdeSandboxparaanálisedemalwaremoderno;

Deveimplementarrecursodemachinelearning,ondeserápermitidoimplementarproteçãoparaum 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.

Deve implementar proteção contra a lista de técnicas/ataques listados no OWASP 10 (Open Web Application security Project)

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.

Teracapacidadedecriaçãodeassinaturasdeataquecustomizáveis.

Teracapacidadedeproteçãoparaataquesdotipo AdobeFlashbinary(AMF)protocol.

Teracapacidadedeproteçãoparaataquesdotipo Botnet.

Teracapacidadedeproteçãoparaataquesdotipo BrowserExploitAgainstSSL/TLS(BEAST).

A solução deve possuir funcionalidade de proteção positiva contra ataques como acesso porforça bruta.

Devesuportardetecçãoaataquesde Clickjacking.

Devesuportardetecçãoaataquesdealteraçãodecookie.

Deveidentificarepreveniratagues dotipo CreditCardTheft.

DeveidentificarepreveniratagueCrossSiteRequestForgery(CSRF).

Asoluçãodevepossuirfuncionalidadedeproteçãopositivacontraataquescomocrosssite scripting (XSS).

Devepossuirproteçãocontraataques de DenialofService(DoS).

Devepossuiracapacidadedeproteçãoparaataques dotipo HTTPheaderoverflow.

Devepossuiracapacidadedeproteçãoparaataques dotipo LocalFileinclusion(FLI).

Devepossuiracapacidadedeproteçãoparaataques dotipo Man-in-the-middle(MITM).

Devepossuiracapacidadedeproteçãoparaataques dotipo RemoteFileInclusion(RFI).

Devepossuiracapacidadedeproteçãoparaataques dotipo ServerInformationLeakage.

Deve possuir proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection).

Devepossuiracapacidadedeproteçãoparaataques dotipo MalformedXML.

DeveIdentificarepreveniratagues dotipo Low-rateDoS.

Devepossuirprevençãocontra SlowPOSTattack.

Deveprotegercontraataques Slowloris.

Devepossuiracapacidadedeproteçãoparaataques dotipo SYNflood.

Devepossuiracapacidadedeproteçãoparaataques dotipo FormsTampering.

A solução deve possuir funcionalidade de proteção positiva contra ataques de manipulação de campo escondido.

Devepossuiracapacidadedeproteçãoparaataques dotipo DirectoryTraversal.

Devepossuiracapacidadedeproteção dotipo AccessRateControl.

Devepossuirahabilidadedeconfigurarproteção dotipo TCPSYNflood-styleparaprevenção de DoS para qualquer política, através de Syn Cookie e Half Open Threshold.

Devepermitirconfigurarregrasdebloqueioamétodos HTTPindesejados.

Devepermitirquesejamconfiguradasregrasdelimitedeuploadportamanhodearquivo.

Devepermitirqueoadministradorbloqueieotráfegodeentradae/outráfegodesaídacombase nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país.

Deve permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem.

Deve permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução.

Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation.

Deve possuir a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP.

Devepossuirafuncionalidadedeprotegerowebsitecontraaçõesdedesfiguração(defacement), com restauração automática e rápida do site caso ocorra à falha.

Devepossuirafuncionalidadedeantivírusparainspeçãodetráfegoearquivos.

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.

DevesercapazdefazeraceleraçãodeSSL,ondeoscertificadosdigitaissãoinstaladosnasolução e as requisições HTTP são enviadas aos servidores sem criptografia.

A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego.

DeveparaSSL/TLSoffloadsuportarnomínimo TLS1.0,1.1,1.2e1.3.

Asoluçãodeveteracapacidadedearmazenarcertificados digitaisdeCA's.

AsoluçãodevesercapazdegerarCSRparaserassinadoporumaCA.

A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL).

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.

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.

Asoluçãodevesercapazdelimitarototaldeconexõespermitidasparacadaservidorrealdeum pool de servidores.

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.

Asolução devepermitir criar regrasdefinindoa ordem em queaspáginasdevem seracessadas para prevenir ataques como cross-site request forgery (CSRF).

AsoluçãodeveteracapacidadededefinirrestriçõesamétodosHTTP.

Asoluçãodeveteracapacidadedeprotegercontraadetecçãodecamposocultos.

Deve permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares.

A solução deve incluir capacidade de atuar como um scanner de vulnerabilidades ou permitir a integraçãocomscannersdevulnerabilidadedeterceirosparadiagnósticoeidentificaçãodeameaças nos servidores web, software desatualizado e potenciais buffers overflows,

Devegerarperfildeproteçãoautomaticamenteapartirderelatórioemformato XMLgeradopor scanner de vulnerabilidade de terceiros.

AsoluçãodevegerarumrelatóriodaanálisedevulnerabilidadesnoformatoHTML.

AsoluçãodevepermitiraexclusãodeURLsnaanálisedevulnerabilidades.

Devesercapazdefazercompressãodeconteúdo HTTP,parareduziraquantidadedeinformações enviadas ao cliente.

Devesuportarredireçãoereescritaderequisiçõeserespostas HTTP.

DevepermitirredirecionarrequisiçõesHTTPparaHTTPS.

DevepermitirreescreveralinhaURLnocabeçalhodeumarequisição HTTP.

Devepermitirreescreverocampo"Host:"nocabeçalhodeumarequisição HTTP.

Devepermitirreescreverocampo"Referer:"nocabeçalhodeumarequisição HTTP.

Devepermitirredirecionarrequisiçõesparaoutrowebsite.

PermitirenviarrespostaHTTP403ForbiddenpararequisiçõesHTTP.

Devepermitirreescreveroparâmetro"Location:"nocabeçalho HTTPdeumarespostade redireção HTTP de um servidor web.

Devepermitirreescreverocorpo("body")deumarespostaHTTPdeumservidorweb.

Devepermitiradicionarocampo X-Forwarded-Forparaidentificaçãodoendereçorealdocliente quando no modo de proxy reverso.

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).

A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizandomecanismoscomoHTMLForm,BasiceSuporteaSSO,métodoscomoLDAPeRADIUSpara consultas e integração dos usuários da aplicação.

Possuircapacidadedecachingparaaceleraçãoweb.

Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.

Devesuportarnomínimo500regrasdereescritaURLdistintas

Devesuportarnomínimo250políticasdeassinaturadistintas

Devesuportarnomínimo500gruposoupoolsdeservidores,ecadapooldevesuportarno mínimo 1000 membros

Devesuportarnomínimo1000IPsvirtuaisconfiguradoseativossimultaneamente

Devesercapazderestringiracessoquandoasrequisiçõesnãotiveremumcabeçalho HTTP específico pré-configurado.

Devesercapazdelimitaronúmerodeusuários/origenssimultâneosacessandoamesma conta/sessão/login.

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.

DevesercapazdeadicionarmúltiplosservidoresADFSemumpooldeservidores

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.

Outrasfuncionalidades

Asoluçãodeveincluirfuncionalidadedebalanceamentodecargaentreservidoresweb.

Devepossuirahabilidadedeconfigurarportasnão-padrãoparaaplicaçãowebHTTPeHTTPS.

Devepossuiracapacidadedebalancear/distribuirtráfegoerotearoconteúdoatravésdevários servidores web.

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

DevesuportaralgoritmoRoundRobinparabalanceamentodecargadeservidores.

DevesuportaralgoritmoWeightedRoundRobinparabalanceamentodecargadeservidores.

DevesuportaralgoritmoLeastConnectionsparabalanceamentodecargadeservidores.

Asoluçãodevesercapazdecriarservidoresvirtuaisquedefinemainterfacederede/bridgee endereço IP por onde o tráfego destinado ao Server Pool é recebido.

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.

DeveserpossívelespecificaronúmeromáximodeconexõesTCPsimultâneasparaumdeterminado servidor membro do Server Pool.

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoTCP.

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoICMPECHO_REQUEST (ping).

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoTCPHalfOpen.

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoTCPSSL.

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoHTTP.

DevepermitirtestededisponibilidadedeservidorwebatravésdométodoHTTPS.

NostestesdedisponibilidadeHTTPeHTTPS,permitirindicaraURLexataasertestada.

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

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

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

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

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

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

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

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

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

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

doCertificadoX509”.

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

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

A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando parâmetros do header HTTP.

A solução deve ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada.

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.

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).

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

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

Asolução ser capazdebalancearassessõesnovas,maspreservar sessõesexistentesno mesmo servidor, implementando persistência baseada em ASP Session ID.

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

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

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

Asoluçãodeve sercapazde enviarcódigode erro503caso ohelth-checkdosservidores estiver desabilitado e/ou o servidor/serviço de retaguarda não estiver responsivo.

DevesuportarFWMARK(marcaçãodetráfego).

ITEM07–SOLUÇÃODESEGURANÇADECOY/HONEYPOT

Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização:VMWarevSphereESXi5.1,5.5ou6.0andlater,KVM,Hyper-V,AWS.AZURE,GCP.Nocasode solução virtualizada a responsabilidade pelo fornecimento de servidor/hardware com licenciamento necessárioserádaCONTRATADA,eoequipamentodeveserinstaladonolocalindicadopelaCONTRATANTE

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.

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

DevesuportaroacessoviaSSHeWEB(HTTPS)paragerenciamentodesoluções

Deveserfornecidatodadocumentaçãotécnica,bemcomomanualdeutilização,emportuguêsdoBrasilou em inglês.

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.

Devesuportarteracapacidademínimade18VMdehoneypot;

Devesuportarnomínimo120VLAN'seestarlicenciadoparanomínimo05VLAN’s;

Devepossuir02(dois)licenciamentoinclusodeWindows7ouWindows10.

Devepossuirlicenciamentopeloperíodode24(vinteequatro)mesesparaasfuncionalidadesde Deception Decoys, AV, IPS, e Web Filtering;

Devesuportaraseguintecombinação:

Windows7, Windows10,Windows10(customizable BYOL), WindowsServer2016and 2019 ou superior

Linux,VPNServer

Medical(PACS,Infusionpump),ERP

IoT,SAPand/orSCADA

Devesuportarosseguintesserviços:

SSLVPN,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,TCPportlistener

Devepossuirascertificações:FCCPart15ClassA,RCM,VCCI,CE,UL/cUL, CB

Deve ser capaz de criar uma rede de máquinas virtuais que se comportam como dispositivos reaisa fimde atrair invasores e monitorar suas atividades na rede.

Devesercapazdemonitorarasaçõesdeatacantesquetentemviolarasmáquinasvirtuais.

Deveanalisarasaçõesdosinvasoresaotentareminvadirasmáquinasvirtuais.

Deve ser capaz de simular serviços, aplicativos ou usuários nas máquinas virtuais a fim de simular um ambiente corporativo real.

Deve possibilitar a instalação de pacote ou script em endpoits reais que simulem interação com osserviçosdasmáquinasvirtuaisafimdeinfluenciarocomportamentodosatacantesaumentandoasuperfície de engano.

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.

O sistema deve ser capaz de demonstrar o número de incidentes por tipo de serviço abrangendo minimamenteosseguintes:SSH,SAMBA,SMB,RDP,HTTP,FTP,TFTP,SNMP,MODBUS,S7COMM,BACNET, IPMI, TRICONEX, GUARDIAN-AST e IEC104.

Devesuportaracriaçãodeperfisdeadministradorparacontrolarosprivilégiosdeacessodoaosrecursosdo sistema. Ao criar uma conta de administrador deve ser atribuído um perfil à conta;

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;

DevesuportaraautenticaçãoremotadeadministradoresusandoservidoresRADIUSeLDAP;

Devesercapazdeserimplantadoemredesdotipoofflineouair-gapped

Devepermitirinseriralicençadeusodoequipamentomesmoemredesdotipoofflineouair-gapped

Devesercapazdeatualizarofirmwaremesmoemredesdotipoofflineouair-gapped;

Devesercapazdeatualizaromódulodesegurançamesmoemredesdotipoofflineouair-gapped;

DevesercapazdearmazenarLognopróprioequipamentoouintegrarcomumservidorremotode armazenamento de log;

Devesuportarservidordelogremotodotiposysloge CEF.

Devepossuirdashboardquemostreinformaçõesdosseguintesitens:

Informaçõesdosistemacomo:Hostname,versãodofirmwareeusuárioconectadonomomento;

Númerodeincidenteeeventoscomsueusníveisdeseveridadeporintervalodetempo;

Númerododecoyimplementado;

PerformancedeCPUeRAM;

Informaçãodeusodedisco;

WidgetdeTopattack;

Devesercapazdecustomizarodashboard;

Devesercapazdeatualizarofirmwareviainterfacegráfica;

Devesercapazderealizarobackuperestoreviainterfacegráfica;

Devesercapazdeconfigurarrotas(camada3OSI);

Devesuportarconfiguraçãodecliente DNS;

DevesuportarconfiguraçãodeIPv4eIPv6;

Devesercapazdecriardiferentesperfisdecontadeadministradordosistema;

DevesercapazdeintegrarcomservidorLDAPeRadius;

DevesuportaraimportaçãodecertificadosCA;

Devesuportaraconfguraçãodeclietedee-mailparaenviodealertas;

Devesercapazdeescolheroníveldeseveridadedoalertaqueseráenviado;

DevesuportarSNMPV1,V2eV3;

Devesuportarconexãocomabasededadosdofabricanteparaatualizarinformaçõesdesegurança;

Devesuportarintegraçãocomsistemadedetecçãodemalware

DevesuportarintegraçãocomSandBox

DevesuportarintegraçãocomNGFWdomesmofabricanteoudeterceiros;

QuandointegradocomsoluçãodeNGFWdevepermitir:

Quarentenardispositivos;

ExibirostatusdeIPbloqueado;

ExportararquivoIOCnoformatoCSVouSTIX;

Mitigareisolardeformaautomáticaendpointinfectadoparaprevinirataquesoumovimentação lateral na rede;

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;

DevesercapazdegerarrelatóriosemPDFou CSV;

Devesercapazdelistarosataquesdetectadoscomasinformaçõesdeseveridade,dataehora, informação do IP do atacante;

Devesercapazdemontarumarepresentaçãodaredeemformademapacontendoinformaçãodo endpoint, decoy e ataque;

Devesercapazdeclassificaronívelderiscodosincidenteseeventos;

Devesercapazdeinformaraquantidadedeeventoseincidentesqueocorreramemumafaixadetempo;

Devesercapazdelistarpelomenosotop5atacantes;

Devesercapazdelistaronúmerodeincidenteporserviçodeformagráfica;

Deve ser capaz de implantar VMs Decoy na rede, para monitorar e ajudar a entender as ações de umatacante ao obter acesso não autorizado ao Decoy;

Devesercapazdeimplementardecoycustomizado(customimage);

DevesuportarimportaçãodeimagemISO;

DevesercapazdecustomizarorecusodeCPU,MemóriaeArmazenamentodaVM-decoy;

ITEM08–SOLUÇAODESEGURANÇADEEMAIL

RequisitosGerais

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;

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.

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.

Devesuportaroroteamentode,nomínimo,3.000.000(trêsmilhões)mensagensporhora;

Suportaroroteamentode,nomínimo,2.500.000(doismilhõesequinhentosmil)mensagensporhora com a análise de anti-spam;

Suportar o roteamento de, no mínimo, 2.000.000 (dois milhões) mensagens por hora com a análise de anti-spam e anti-vírus;

Permitiraconfiguraçãode,nomínimo,2.000(doismil)domínios;

Permitiraconfiguraçãode,nomínimo, 40.000(quarentamil)mailboxesquandooperandoemmodo gateway.

FuncionalidadesGerais

Asolução devepossuireestarlicenciada comfuncionalidadesdeanti-spam, anti-vírus, anti-spyware e anti-phishing. deve ser capaz de realizar a inspeção de correio da Internet de entrada e saída.

DevepermitirintegraçãocomoMicrosoft365atravésdeAPI;

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;

Devepossuirumassistente(wizard)paraoprovisionamentofácilerápidodeconfiguraçõesbásicase domínios para proteção.

Deve se conectar em tempo real com a base de dados do fabricante para baixar atualizações anti- spam.

Deveoferecerproteçãocontra-ataquesdenegaçãodeserviçocomo,porexemplo,MailBomb.

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.

Devesercapazdeentregarocorreiobaseadoemusuáriosexistentesemumabase LDAP.

Devesuportarquarentenaporusuário,possibilitandoquecadausuáriopossaadministrarsuaprópria 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.

Devesercapazdeagendaroenvioderelatóriosdequarentena.

Devesercapazderealizaro armazenamentodee-mails(archiving)baseadonaspolíticasde envio e recepção, com suporte também a armazenamento remoto.

Devesercapazdemanterfilasdecorreio(queue)emcasodefalhanaconexãodesaída,atrasos ou erros de entrega.

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.

Deveteracapacidadedeavaliar,retere/oubloqueare-mailsquetêmameaçasavançadas,como dia-zero, através da análise com sandboxing.

Devesercapazdefiltraranexoseconteúdodee-mails.

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.

Deve ser capaz de filtrar e-mails baseados nos URI's (Uniform Resource Identifier) contidos no corpo da mensagem.

DevesercapazderealizaranálisedeimagemedocumentosPDFparaaprocuradespam.

DevesuportardirecionamentoemIPv4eIPv6.

Devesuportargreylistparacontasdee-mailemIPv4eIPv6.devesercapazdedetectar endereços IP forjados (Forged IP).

Deve ser capaz de funcionar como gateway, atuando como MTA (Mail Transfer Agent). devesuportar Sender Policy Framework (SPF).

DevesuportarDomainKeysIdentifiedMail(DKIM).

DevesuportarDomainBasedMessageAuthentication(DMARC).

Deve ser capaz de atrasar o envio de e-mail de grandes dimensões para os horários que são de menos carga.

Deve ser capaz de definir o encaminhamento de correio (relay) para um IP específico baseado no IP de origem da mensagem.

Devepermitiroarmazenamentodee-mailsequarentenalocalmenteouemservidorremoto.

Devepermitirsuaconfiguraçãoatravésdeinterfaceparaacessoà Web(HTTP,HTTPS).

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.

Devesercapazdefornecer,pelomenos02(dois)níveisdeacessodegestão:

Leitura/Gravação(Read/Write)ouSomenteLeitura(ReadOnly).

Deve ser capaz de armazenar logs e eventos localmente e também enviá-los para servidoresremotos (Syslog).

Devepermitirorelatodeatividades,analisandoosarquivosdeeventos(logs)eapresentá-losna tabela ou formato gráfico.

Quandoa soluçãoestiverimplementadaemaltadisponibilidade,devesercapazdemonitoraro status do link.

Quando a solução estiver implementada em alta disponibilidade, deve suportar o failover derede.

Quandoasoluçãoestiverimplementadaemaltadisponibilidade,devesuportaromodo ativo/passivo.

FuncionalidadesdeDLP

AfuncionalidadedeDLPdevepermitirespecificarainformaçãoaserdetectadacomopalavras,frases e expressões regulares.

Deve possuir uma lista predefinida de tipos de informações, como números de cartão de crédito e outros.

Devepermitiracriaçãoearmazenamentodeimpressõesdigitais(fingerprint)dedocumentos.

Devepermitiracriaçãodefiltrosporarquivo.

Devepermitirageraçãoearmazenamentodeimpressõesdigitais(fingerprint)de anexoseme-mail.

FuncionalidadesdeIBE

A solução deve suportar criptografia das mensagens baseada em identidade (Identity Based EncryptionIBE)paraqueodestinatárionãorequeiraumaPSKoucertificadoinstaladoanteriormente para a descriptografia.

DevepossuirlicençasEmailDataLossPrevention,URLClickProtectioneCloudSandboxing;

AcriptografiademensagenscomIBEdevesuportartantoométodopush,quantoométodopull,em que a mensagem criptografada é armazenada na plataforma de e-mail para acesso remoto autenticado ou ser enviada como anexo para o destinatário.

Emambos métodosdacriptografiaIBE,deveterum registrodousuáriododestinonaplataformade e-mail, de modo que, para ver as mensagens criptografadas, um processo de autenticação seja necessário.

SuporteaRFC's

AsoluçãodevesuportarasseguintesRFC's(RequestForComments):

CriptografiaSMTPSeSMTPover TLS;

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);

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

RFC3464(ExtensibleMessageFormatforDeliveryStatusNotifications);RFC4954(SMTPService Extension for Authentication);

RFC5321(SMTP);

RFC6376(DomainKeysIdentifiedMail(DKIM)Signatures);

RFC6522(Multipart/ReportContentTypefortheReportingofMailSystemAdministrative Messages);

RFC7208(SenderPolicyFramework(SPF)forAuthorizingUseofDomainsinE-Mail);

RFC2221(LoginReferrals);

RFC2342(IMAP4Namespace);

RFC2683(IMAP4ImplementationRecommendations);RFC2971(IMAP4IDExtension);

RFC3348(IMAP4ChildMailboxExtension);RFC3501(IMAP4rev1);

RFC3502(IMAPMultiappendExtension);

RFC3516(IMAP4BinaryContentExtension);RFC3691(UnselectCommand);

RFC4315(UIDPLUSExtension);RFC4469(CatenateExtension);

RFC4731(Extension toSEARCHCommandforControllingWhat KindofInformation IsReturned);

RFC4959(ExtensionforSimpleAuthenticationandSecurityLayer(SASL)InitialClientResponse);

RFC5032(WITHINSearchExtension);RFC5161(EnableExtension);

RFC5182(ExtensionforReferencingtheLastSEARCHResult);RFC5255(IMAPInternationalization);

RFC5256(SortandThreadExtensions);RFC5258(ListCommandExtensions);RFC5267(Contexts for IMAP4);

RFC5819(ExtensionforReturningSTATUSInformationinExtendedLIST);RFC6154(LIST Extension for Special-Use Mailboxes);

RFC6851(MOVEExtension);

RFC7162(IMAPExtensions:QuickFlagChangesResynchronization(CONDSTOR)andQuick Mailbox Resynchronization (QRESYNC));

RFC1939(POP3);

RFC2449(POP3ExtensionMechanism);

RFC1155(StructureandIdentificationofManagementInformationforTCP/IP-basedInterface);

RFC1157(SNMPv1);RFC1213(MIB 2);

RFC2578(StructureofManagementInformationVersion2);RFC2579(TextualConventionsfor SMIv2);

RFC2595(UsingTLSwithIMAP,POP3andACAP);RFC3410(SNMPv3);

RFC3416(SNMPv2).

ITEM09–SERVIÇOSPROFISSIONAISDEMONITORAMENTOESEGURANÇADODATACENTERDAPRODEB

CARACTERISTICASGERAIS

A CONTRATADA deve prestar durante a vigência contratual de 24 (vinte e quatro) meses, serviços profissionais, especializadose multidisciplinarespara omonitoramentoea proteçãodoambientede datacenterdaPRODEB,incluindoGestãodeVulnerabilidades,GestãodeIncidentes,Monitoramento e Visibilidade de ataques Cibernéticos, Operação e Atendimento de Requisições, Testes de Invasão, Simulação de ataques relacionados à Segurança Digital;

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, açõesproativasvoltadaspara a segurança doparquecomputacional da PRODEB afimdeemantê-lo estável, disponível e integro;

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

Noprazodeaté30(trinta)diasapós aemissãodaOrdemdeServiço,aCONTRATADAdeverárealizar 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 SystemsSecurity, queserá responsável pela apresentação dosresultadosda análiseao gestor, fiscais do contrato e gestores da PRODEB;

3.9.1.4.3.Deveráfornecerosresultadosdaanáliseparaaequipetécnicada CONTRATANTE;

PRINCIPAISATIVIDADES A SEREMEXECUTADAS DE FORMACONTÍNUA PELA CONTRATADA:

Interagir com a equipe de Segurança da PRODEB de forma contínua para otimização das ações deproteçãodoambiente,definiçãodeprocessos,procedimentosoperacionaiseinstruçõesdetrabalho;

Acompanharaexecuçãodosserviçosparaocumprimentodosníveisdeserviçoestabelecidos;

Priorizar osatendimentoscríticos,conformedefiniçãodoCONTRATANTE;

Monitorar permanentee avaliarcriticamenteos produtoseserviços desegurançado CONTRATANTE;

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;

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

ReagiraoseventosdeSegurança daInformaçãoquepossamafetara disponibilidade, integridadeou confidencialidade das informações existentes nos sistemas ou serviços de TI do CONTRATANTE;

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.

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

Supervisionarsuaequipenaexecuçãodosserviços;

Elaborareproporplanodeexecuçãodosserviços;

Organizaraalocaçãodeturnosedeprofissionaisdesuaequipe;

Definirplanodetreinamentoinicialecontínuodosprofissionaisqueexecutamosserviços;

ExecutaroutrosserviçoscorrelatosàsupervisãodosprofissionaisnaexecuçãodosServiços;

Orientaraatuaçãodaequipetécnicaemsituaçõescríticasdetrabalho,bemcomointeragircom a Equipe de Segurança da PRODEB;

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;

Receberasdemandasdosserviçosrelativasàáreadesegurançadainformaçãoeprovidenciara execução e alocação de recursos de trabalho;

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

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;

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

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

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

Sugerirnovastecnologiasparamodernizaroambientetecnológico,buscandosubsidiaraequipe do CONTRATANTE na gestão de segurança da informação;

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.

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

Consolidarassugestõesdemelhoria;

ReceberasdiretrizesrelacionadasàáreadeSegurançadaInformaçãoeprovidenciaraexecução e alocação de recursos de trabalho;

Apoiareparticiparnaimplementaçãodosprocessosbemcomonamensuração dos indicadoresdeobjetivosinstituídospelo CONTRATANTE;

Realizar as atividades em estrita observância na Política de Segurança da Informação e demais normasestipuladas pelo CONTRATANTE;

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 ANEXOIII–SOLUÇÕESDESEGURANÇA,paraapresentaçãoaoCONTRATANTE,constandoasmedidas tomadas e sugestões;

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

Auxiliarnaelaboraçãodosprocedimentosemetodologias,everificarereportarocumprimento dos mesmos pelas demais áreas de TI;

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

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

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

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;

Participar,quandosolicitado,daimplantaçãodeprojetos/soluções,substituiçãoeatualizaçãode soluções destinadas à Segurança da Infraestrutura de rede;

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

Monitorareanalisaroslogsdosserviçosdesegurança(equipamentos,sistemas operacionaisde servidoreseclientes,conexões,programasutilizadosetc.),propondoaçõescorretivasedemelhorias;

Execuçãodemudançasdeconfiguraçãonosativossobsua administração;

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

Osserviçosdevemsercapazesdegarantiramelhorutilizaçãopossíveldosrecursosdesegurança existentes na empresa, bem como responder de forma efetiva a eventuais incidentes de segurança.

Osserviçosdeveminclui,masnãoselimitarão a:

Gerenciamento de Soluções de Segurança Existentes: Gerenciamento de todas as soluçõesdesegurançaatualmenteimplementadasnaPRODEB.Issoincluia 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.

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.

GestãodeVulnerabilidades:Identificaçãoemitigaçãodevulnerabilidadesnoambiente de datacenter. Isso inclui a realização de avaliações de vulnerabilidade.

Simulação de Violação e Ataque: Implementação de simulações de violação e ataque paratestaraeficáciadasmedidasdesegurançaexistenteseidentificaráreasdemelhoria.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.

GestãodeIncidentesdeSegurança:Respostarápidaeeficazaincidentesdesegurança para minimizar o impacto e garantir a recuperação rápida do sistema.

Segurança Operacional: Implementação de controles de acesso robustos para garantir que apenas indivíduos autorizados tenham acesso ao ambiente de datacenter. Todas as operaçõesrealizadasnoambienteoperacional da PRODEB,seja localou remotamente, devem ser gravadas e passíveis de auditoria.

Automação e Integração de Segurança: Implementação de automação e integração entre asdiferentes soluçõesdesegurança para otimizar a resposta a incidentes. Isso permitirá umarespostamaisrápidaeeficazaincidentesdesegurança,minimizandooimpactopotencial e melhorando a eficiência operacional;

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.

Todososprofissionaisenvolvidosealocadosparaaprestaçãodosserviços,deverãoter vínculo formal com a empresa CONTRATADA.

AMBIENTEDACONTRATANTEPRODEB

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

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

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.

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.

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.

ESCOPODOSSERVIÇOSDESUPORTEEMONITORAMENTO

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.

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;

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;

Osserviçosdeoperação,configuraçãoeatendinentoàsmudançaserequisiçõesdizemrespeito
enãoselimitama:aaplicaçãoderegras,políticas,configurações,exceções,execuçãodescripts
eprocedimentos,execuçãoderefasestabelecidasnofluxodemudança,solicitaçõesenviadas
pelasequipeseclientesdaCONTRATANTEnassoluçõeseprodutosdesegurançainstaladosno Datacenter da CONTRATANTE;

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;

Osserviçosdeintegraçãoeautomatizaçãosereferem, enãoselimitama,realizarpor meiode 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 açõesderespostasapossíveisincidentescomatuaçãoimediataindependentedeumoperador humano;

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 deinteiraresponsabilidadedaCONTRATADAe nãodeverágerarônusàCONTRATANTE;

Todos os equipamentos e softwares ofertados pela CONTRATADA, quando for o caso, e necessário à consecuçãodasatividadesdesegurança,devematenderàsespecificaçõestécnicasdoobjetodurante 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);

Todososequipamentos,quandoforocasoenecessárioàprestaçãodosserviços,devemsernovose 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 dofabricante,ouseja,nãopodemterprevisãodedescontinuidadedefornecimento,suporteouvida;

Os softwares ofertados pela CONTRATADA devem ser instalados em sua versão mais estável e atualizadaeestarcobertosporcontratosdesuporteeatualizaçãodeversãodofabricantedurantea 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;

Oconjuntoderequisitosespecificadosparacadaserviçopode seratendidopormeiodecomposição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desdequenão impliquealteração da topologia deredeou na exposição deativosa riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade;

Paraquesejapossíveloacompanhamento,auditoriaedirecionamentodeaçõesnoambientedeverá 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.paraquesejapossíveloacompanhamento,auditoriaedirecionamentodeaçõesno ambiente;

Todos os hardware/software a serem utilizados para atendimento às exigências de serviços deste TermodeReferênciadeverãoserapresentadosdeformaclaranapropostacomercialedeverãoestar acompanhados de comprovação técnica através de documentação oficial e pública emitida pelo fabricante das soluções;

ACONTRATADAdeverádisponibilizaràCONTRATANTE,PainelCentraldeInformaçõeseGerência das Soluções, permitindo monitorar em conjunto com o Centro de Operação de Segurança da InformaçãodaCONTRATANTE quedevemocorrer24x7emregimeremoto. Éderesponsabilidadeda CONTRATADA manter as informações do Painel Central sempre atualizadas e em operação.

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

Este serviço deverá monitorar e gerenciar e integrar as soluções de segurança da informação elencadasnesteTermodeReferência, bemcomoassuasatualizaçõesduranteoperíododevigência de contrato.

ACONTRATADAdeveráavaliarsituaçõesemqueoambienteestejasobataqueouriscoiminente de ataque,provendo o conhecimento e experiência necessários para recomendar possíveismedidas de preparação, mitigação, contenção, defesa e resposta.

Osserviçoscomportarãomonitoramento,operação,atendimentoderequisições,administração e suporte de todos as soluções elencadas neste Termo de Referência.

ACONTRATADAseráresponsávelporapoiaroprocessodeRespostaaIncidentesdeSegurança.

ACONTRATADAdeveráproduzirrelatóriosdeIncidentesdeSegurança.

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.

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

Oacessoaocentrodeoperaçõeseàssoluçõesda CONTRATADAeda CONTRATANTEdevemser restrito apenas a funcionários autorizados.

A CONTRATADA deverá manter atualizados os softwares destinados à execução dos serviços, implementandoasúltimasversõesestáveis,atualizaçõesecorreçõesrecomendadaspelofabricante, de modo a assegurar a plena integridade, segurança e o desempenho do ambiente em produção.

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

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.

A CONTRATADA deverá disponibilizar à CONTRATANTE serviço para abertura e acompanhamentoderequisições,mudançaseincidentesquedeveráestaracessíveldurante24horas

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

Serviçodeatendimentocomdiscagemgratuita(0800)eoudecustolocalparatelefone fixo (DDD 71).

E-mail.

Aberturadeticketatravéssoluçãodegestãodeincidentesda CONTRATADA.

Nãohaverálimitaçãononúmerodechamadosquepoderãoserabertos.

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

Númerosequencialdaordem. 3.9.4.25.2. Data e hora de abertura.

Severidade.

Descrição do problema. 3.9.4.25.5. Itemdeconfiguraçãoassociado

3.9.4.25.6. Responsável pela abertura do chamado 3.9.4.25.7. Responsávelpeloatendimentodochamado

3.9.4.25.8. Tipodochamado(requisição,incidenteourequisiçãodemudança) 3.9.4.25.9. Data e hora do início do atendimento.

3.9.4.25.10. Dataehoradetérminodoatendimento(solução) 3.9.4.25.11. Auditoria de todo o fluxo e atendimentos feitos;

Omonitoramentodedisponibilidadedosativosdoambientedo CONTRATANTE,elencadosneste Termo de Referência, deverá ser realizado através de ferramenta (hardware e/ou software) que coletaráasinformaçõesnecessáriasparagarantirqueassoluçõesestejamsempreativaseoperantes.

Deveserelaboradoeenviadomensalmenteumrelatórioexecutivocomoresumodasprincipais ocorrênciaseasprovidênciasexecutadaspelaCONTRATADA,alémdegráficos eestatísticasrelativos àconformidadeoperacionaldoambiente.Aformataçãodesterelatóriodeveestaremcomumacordo com a CONTRATANTE.

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:

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.

Quanto às atualizações pertinentes aos softwares, entende-se como “atualização” a aplicaçãodetodaequalquerevoluçãodesoftware,incluindocorreções,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.

Para servidores, a CONTRATADA deverá manter índice de atualização do conteúdo de segurança(ex:assinaturas)eengines/motoresdedetecçãodeEPPeEDRacimade100%,desde quesuportadaspelosistemaoperacionaldoendpointequeoacessoàsmáquinassejafacultado à CONTRATADA pela CONTRATANTE. Este indicador deve ser extraído da própria console de gerenciamento da solução.

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.

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

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.

AssolicitaçõesdealteraçãodeconfiguraçõesdeverãoserrealizadasconformeoANSdefinidona Seção – Acordo de Nível de Serviço – ANS.

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, preferencialmenteemferiadosefinaisdesemana.Nenhumaaçãopoderáserexecutadanoambiente sem a ciência e anuência do CONTRATANTE.

ACONTRATADAdeveráseguiroprocessodemudançaestabelecidopeloCONTRATANTE.Sempre quesolicitado,aCONTRATADAdeverá estardisponívelparaparticipardasreuniõescomoComitêde Mudanças, para prestar informações sobre os ambientes e serviços por elas executados.

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.

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.

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.

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.

ACONTRATADAdeverácomunicarformalmenteoCONTRATANTEsemprequeidentificar algum serviço com falhas de implementação e que tornem o ambiente vulnerável a indisponibilidade.

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

Osserviçosdemonitoramento,suportetécnico,manutençãoerespostaaincidentesdeveráser prestado por profissional devidamente certificado nas soluçõestecnológicaselencadas neste Termo de Referência.

ACONTRATADAdeverácontarcomfuncionárioscapacitadosparaarealizaçãodasatividadesde monitoramento de redes e análise e resposta a incidentes de segurança, conforme quadro mínimo de pessoal e certificações exigidas neste TR.

Caso a Equipe de Atendimento Técnico da CONTRATADA sofra alguma alteração em sua composiçãoduranteavigênciadestecontrato,talfatodeveserimediatamenteinformadoaogestor 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.

AsinformaçõesrelacionadasaoANSestãonaSeção–AcordodeNíveldeServiço–ANS.

Ao final, ou em qualquer hipótese de encerramento antecipado do contrato, a CONTRATADA deverárepassaràCONTRATANTEtodooconhecimentotécnicoedeprocessosutilizadosnaprestação 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.

SERVIÇOSDEGESTÃODEVULNERABILIDADES

Serviço de gestão de vulnerabilidades tem por objetivo Serviço de gestão de vulnerabilidades, que temporobjetivo,deformaproativaerecorrente,identificarpossíveisvulnerabilidadesdesegurança da informação no ambiente a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas;

No início da atuação da CONTRATADA, em até 30 dias após a emissão da Ordem de Serviço, deverá realizarumdiagnósticoinicialdasvulnerabilidadesexistentes,utilizandoassoluçõesdisponibilizadas 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.

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.

A CONTRATADA deverá realizar checagens (scans) e varreduras nos ativos, aplicações, servidores e recursos da CONTRATANTE. A CONTRATANTE será responsável pelo tratamento contínuo das vulnerabilidadesencontradasnainfraestruturaeaplicaçõesdaPRODEB,comoapoiodasinformações para correção geradas pela CONTRATADA.

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.

Apósanálisede falsopositivo, a CONTRATADAdeverá informar à CONTRATANTE asvulnerabilidades encontradaseosmeiosdemitigaçãodestasvulnerabilidades,inclusivesoluçõesdecontornoquando não houver soluções conhecidas.

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.

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.

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

Denominação	Formade Cálculo	Filtro	Agrupador	Descrição
Quantitativo de vulnerabilidades	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	Númerototalde vulnerabilidades
Quantitativo de vulnerabilidades críticas por área responsável	Soma de vulnerabilidades críticas por área responsável	Vulnerabilidades críticas	Vulnerabilidades	Númerototalde vulnerabilidades críticas por área responsável
Quantitativo de vulnerabilidades corrigidas	Soma de vulnerabilidades corrigidas	Vulnerabilidades corrigidas	Vulnerabilidades	Númerototalde vulnerabilidades corrigidas
Quantitativo de vulnerabilidadesem Aplicações WEB	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	Númerototalde vulnerabilidades em Aplicações WEB
Quantitativo de vulnerabilidades corrigidas em aplicações WEB	Soma de vulnerabilidades corrigidas em aplicações WEB	Vulnerabilidades corrigidas em aplicações WEB	Vulnerabilidades	Númerototalde vulnerabilidades corrigidas em Aplicações WEB
Quantitativo de vulnerabilidadesem ativos	Soma de vulnerabilidades em ativos	Vulnerabilidades em ativos	Vulnerabilidades	Númerototalde vulnerabilidades em ativos
Quantitativo de vulnerabilidades corrigidasemativos	Soma de vulnerabilidades corrigidas em ativos	Vulnerabilidades corrigidas em ativos	Vulnerabilidades	Númerototalde vulnerabilidades corrigidas em ativos
Quantidade de vulnerabilidades em códigosde aplicações	Soma de vulnerabilidades emcódigosde aplicações	Vulnerabilidades em códigos de aplicações	Vulnerabilidades	Númerototalde vulnerabilidades emcódigosde aplicações
Quantitativo de certificadosdigitais expirados	Soma de certificados digitais expirados	Certificados digitaisexpirados	Certificados digitais	Número total de certificados digitaisexpirados
Quantitativo de certificadosdigitaisa expirar em 3 meses	Soma de certificados digitaisaexpirar em 3 meses	Certificados digitaisaexpirar em 3 meses	Certificados digitais	Númerototalde certificados digitaisaexpirar em 3 meses

Denominação	Formade Cálculo	Filtro	Agrupador	Descrição
TOP10– Ativosmais vulneráveis	Soma de vulnerabilidades por ativo	Vulnerabilidades por ativo	Vulnerabilidades	TOP10do número de vulnerabilidades por ativo
TOP10– Aplicações WEB mais vulneráveis	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP10do número total de vulnerabilidades em Aplicações WEB
TOP10– Aplicações WEB mais vulneráveis em comparação com OWASP	Soma de vulnerabilidades em Aplicações WEB em comparaçãocom OWASP	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP10do número total de vulnerabilidades em Aplicações WEB em comparaçãocom OWASP

OprocessodescritoéomínimoesperadoaserseguidoeexecutadopelaCONTRATADAtodaviacomo 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.

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.

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

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;

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;

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.

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 maisprincípiosbásicosdeSegurançadaInformação:Confidencialidade,Integridade,Disponibilidade e Privacidade.

O serviço de resposta a incidentes será responsável por monitorar equipamentos e softwares componentesdassoluçõesdesegurançadaCONTRATANTE,envolvendoidentificação,classificaçãoe análise de eventos que possam comprometer a disponibilidade, integridade, confidencialidade dos serviços e requerimentos legais de privacidade dos serviços.

ACONTRATADAdeveráproverserviçosderespostaaosincidentesdesegurançadainformaçãodiante os eventos registrados no monitoramento.

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.

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

O monitoramento de segurança deverá ser autônomo (automatizado) e realizado através de ferramentaspróprias daCONTRATANTEintegradasviaAPIcomasconsoles/servidoresde

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

A ocorrência de alertas de alta criticidade devem acionar diretamente, de forma automática, através de alarmes no 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.

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).

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.

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.

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.

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

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.

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.

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

OsdadosdeSLAdotratamentodeincidentes,incluindooSLAdecadaumadesuasetapas,deve ser disponibilizado em tempo real para a contratada através de dashboards gráficos.

Oprocessodetratamentodeincidentesdeveconterpelomenosasseguintescaracterísticas:

NotificaçãoautomáticaeimediatadaCONTRATADAsobreaocorrênciadetectada. 3.9.6.19.3. Abertura

3.9.6.19.4. Investigaçãodaocorrênciaatravésdosrecursosfornecidospelasolução. 3.9.6.19.5. Determinação da real criticidade do incidente.

3.9.6.19.6. Execuçãodeaçõesdecontençãopreviamenteacordadascomocliente.

Oprocessoautomatizadodevesercapazdetratardeformadiferenciadapelomenos4níveisde criticidade de alertas.

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.

Oprocessoautomatizadodevesercapazdeemitiravisossonorosatravésdeaplicativodecelular para os técnicos da CONTRATADA e da CONTRATANTE, com diferentes graus de intensidade a depender do nível de criticidade da situação detectada.

Devepermitiracustomização,paracadasoluçãodaCONTRATANTE,dequaistiposdealertasse enquadram em cada um dos níveis de criticidade.

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

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

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

Tabeladeatrasomédiodetarefasjáencerradas.

Tabeladetempomédiodeexecuçãodetarefasjáencerradas.

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.

Além do monitoramento da ferramenta de análise avançada de logs e pacotes de rede, a CONTRATADAdeverá realizar omonitoramento deloge eventosde segurança das soluçõesde 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.

Paraexecuçãodoserviço,aCONTRATADA seráresponsável pelaintegração,pormeiodacoleta 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

Apósoincidentedesegurançaaberto,seráderesponsabilidadedogrupoderespostaaincidente de segurança da CONTRATADA, analisar os logs e artefatos enviados, a fim de no primeiro instante identificar as fontes geradoras de tais logs.

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.

Como próximo passo o grupo de resposta a incidente de segurança da CONTRATADA, deverá comunicaraotimedesegurançadainformaçãodoCONTRATANTE,deacordocomosSLAsinformados 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:

Prioridade:Representação/número deprioridadeou severidadedo incidente, emuma escala de 1 a 4 sendo 1 a maior prioridade.

Categoria/Classificação:Palavraúnicaqueclassificaotipodoincidente,comomalware, phishing, misconfiguration entre outros.

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.

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.

Açõesrecomendadas:Instruçõesinteligentesesimplesaseremseguidasquedetalhem 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.

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.

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 atravésda combinação deurgênciae impacto, ondeimpacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente.

Apósanálisesiniciaisdoincidente,caberáaogrupoderespostaaincidentedesegurança,realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

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.

Umavezidentificadoocomportamentoeosprincipaisvetoresdeataque,ogrupoderespostaa incidentedesegurançadaCONTRATADA,deverádefinirumaestratégiaparaamitigaçãoecontenção doataqueemquestão.Casosejanecessárioqualquer tipodealteraçãonoparquecomputacionaldo CONTRATANTE, para contenção e mitigação do incidente, deverá obedecer aos níveis de autonomia da CONTRATADA definidos no início do contrato.

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 dosserviçosafetados. Tais evidênciasserãoutilizadasatéa finalizaçãodo processo, para execução de análise forense do caso.

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

Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciaro 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.

Olaudodeveráconter,alémdasinformaçõestécnicasdoincidente,asuaclassificaçãoconforme a tabela a seguir:

PERSPECTIVA	CLASSE	DESCRIÇÃO

Quantoa Natureza	Evento	AlgoqueocorreunosSistemasdeInformações, Infraestrutura ou Dados,masnãoénecessariamentemalicioso ou que requer uma ação.
	Alerta	Algopotencialmenteacionável.Umaindicação de um evento acionável.
	Incidente	Qualquer evento com a violação da confidencialidade, integridade, disponibilidadeeprivacidade,mas**sem impacto à missão ou ao negóciodaorganização.**
	IncidenteGrave	Qualquer evento com violação da confidencialidade, integridade, disponibilidadeeprivacidade,**comimpactoà missão ou ao negócio.**
	Invasãoe/ou Vazamento	Perdaoucomprometimentodesistemas, dados regulados, ou de propriedadeempresarialquedisparaumaação ou resposta legal queváalémdosserviçosdemonitoramentoe resposta a incidentes.
Quanto ao Impactode Negócio	Nenhum	Nenhumefeitonacapacidadedaorganização de oferecer todososserviçosatodososusuários.
	Baixo	Efeitomínimo;aorganizaçãoaindapode fornecer todos os serviçoscríticosatodososusuários,mas perdeu eficiência.
	Médio	Aorganizaçãoperdeuacapacidadedefornecer um serviço essencialecríticoparaumsubconjuntode usuários do sistema.
	Alto	Aorganizaçãonãoémaiscapazdefornecer alguns serviços essenciaisecríticosanenhumusuárioe/ou houve comprometimentodedadosinstitucionais e/ou pessoais.

	Crítico	Aorganizaçãonãoémaiscapazdefornecer alguns serviços essenciaisecríticosanenhumusuárioe/ou houve comprometimentodedadosinstitucionais e/ou pessoais.
Quanto ao Impacto de Informações	Nenhum	Nenhumainformaçãofoiexfiltrada,alterada, apagada ou, de qualqueroutraforma,comprometida
	Quebra de Privacidade	Informaçõessensíveispessoalmente identificáveis (PII), foram acessadasouexfiltradas.
	Quebra de Propriedade	Informaçõesproprietáriasnãoclassificadas, tais como informações deinfraestruturacríticaprotegida(PCII),foram acessadas ou exfiltradas
	Perdade Integridade	Informaçõessensíveisouproprietáriasforam alteradasouexcluídas
	Quebra de Privacidade	Informaçõessensíveispessoalmente identificáveis (PII), foram acessadasouexfiltradas.

	Quebra de Propriedade	Informaçõesproprietáriasnãoclassificadas, tais como informações deinfraestruturacríticaprotegida(PCII),foram acessadas ou exfiltradas
	Perda de Integridade	Informaçõessensíveisouproprietáriasforam alteradas ou excluídas.
	Quebra de Privacidade	Informaçõessensíveispessoalmente identificáveis (PII), foram acessadasouexfiltradas.
Quanto ao Impacto de Recuperação	N/A	Nãose aplica
	Regular	Otempopararecuperaçãoéprevisívelcomos recursos existentes.
	Complementado	Otempopararecuperaçãoéprevisívelcom recursos adicionais.
	Estendido	Otempopararecuperaçãoéimprevisível;são necessários recursosadicionaiseajudaexterna.
	Não Recuperável	Arecuperaçãodoincidentenãoépossível(por exemplo, os dadossensíveisexfiltradossãopublicados; lançar investigaçãoparaapuraçãocrimina

Ogrupoderespostaaincidentedesegurançada CONTRATADA,devedocumentarnaferramenta 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.

Oprocessodescritoéomínimoesperadoaserseguidoeexecutado pelaCONTRATADA,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.

SERVIÇOSDEINTEGRAÇÃODEINFORMAÇÕESDEINTELIGÊNCIASOBREAMEAÇAS(THREATINTELLIGENCE):

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,internetprofunda(deepweb),spam,ataquesAPT(advancedpersistentthreats), ransomware etc.;

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

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;

Monitorar ameaças emergentes e avaliar a aplicabilidade especificamente no ambiente do CONTRATANTE, propondoproativamentea realizaçãode contramedidascomo objetivo deprevenir a exploração de alguma brecha de segurança;

A solução deve ser capaz dedetectar emtempo real, ameaçasalimentadaspelas seguintesbases de inteligência:

relatóriosdeameaçasesegurança;

relatóriosdebotnetsecentrosdeComandoeControle;

identificaçãodeexploitkits;

indicadoresdeataques"zeroday";

indicadoresdecomprometimento,suspeitaseavisosInformativos;

inteligênciadetendências;

proxiesanônimos;

classificaçãodesites;

endereçosderedeTOR

SERVIÇOSDEVALIDAÇÃOCONTÍNUADESEGURANÇA

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.

ACONTRATADAdeveráfornecerumserviçodeValidaçãodeControledeSegurança.Esteserviçodeve 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.

A CONTRATADA deverá fornecer um serviço que simula ameaças cibernéticas do mundo real para identificarlacunas deprevençãoedetecção.Esteserviçodeveincluiraobtençãoderecomendações de mitigação acionáveis para abordá-las de forma rápida e eficaz.

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.

ACONTRATADAdeveráfornecerumserviçoquetestaaprontidãodesegurançacontramaisde3.800 ameaças, incluindo malware, ransomware e APTs.

ACONTRATADAdeveráfornecerumserviçoquevalidaapreparaçãocontraasúltimasameaças.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.

ACONTRATADAdeveráfornecerumserviçoquemapeiaosresultadosdaavaliaçãoparaoFramework MITRE ATT&CK, permitindo a visualização da cobertura de ameaças e a priorização da mitigação de lacunas.

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

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.

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.

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.

ACONTRATADAdeveráfornecerumserviçodeconsultoriaparafornecerconselhosdemitigação parabrechasdesegurançaidentificadas.Esteserviçodeveincluiraanálisedeincidentesdesegurança e a recomendação de medidas de mitigação.

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

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.

ACONTRATADAdeveráfornecerumserviçodesimulaçãodeataquescibernéticosparaavaliara 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.

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.

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.

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.

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.

A CONTRATADA deverá fornecer um serviço de teste da eficácia de segurança dos sistemas de segurançadecliente,rede,virtualizaçãoenuvemdainstituição.Esteserviçodeveincluirarealização de testes para avaliar a eficácia das medidas de segurança em diferentes sistemas e ambientes.

A CONTRATADA deverá fornecer um serviço de avaliação do nível de segurança fornecido por umgrupodeendpointse/ou tecnologiasdesegurança derede.Esteserviçodeveincluir a realização de avaliações para determinar a eficácia das medidas de segurança em proteger os endpoints e a rede.

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.

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.

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)eEndpointDetectionandResponse(EDR).Esteserviçodeveincluiracapacidadedeanalisara eficácia das soluções SIEM e EDR na detecção e alerta de ameaças.

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.

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

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

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.

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.

Asolução devefornecer acesso à coberturado framework MITRE ATT&CKna interface web para cada simulação.

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.

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.

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 integradasaoutrossistemasdesegurança,independentementedofornecedoreda tecnologia subjacentes.

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.

Os componentes da solução devem executar simulações de ataque entre seus componentesenãodeveminiciarconexõescomnenhumaaplicaçãodeproduçãoesistemade endpoint para fornecer uma avaliação sem riscos, a menos que configurado para movimento lateral.

Asavaliaçõesdecontroledesegurançadeterminaldevemserrestritas 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.

Asoluçãodeverásuportaraintegraçãoecomunicarcomoutrassoluçõesbaseadasnum acesso “Application Programming Interface” (API) ou no protocolo Syslog para fins como:Relatóriospersonalizados,Painéispersonalizadose Integraçãocomsoluçõesdeterceiros como SOAR, SIEM ou outras plataformas.

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

Asoluçãodevefornecertemplatesdeameaçasestáticosprontosparausoparaameaças emergentes e sugeridas que o usuário também pode modificar para necessidades personalizadas.

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.

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

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.

Asoluçãodevesercapazdeadicionarautomaticamenteataquesrecém-adicionadosaos templates dinâmicos sem intervenção do usuário.

A solução deve usar payloads de ataques maliciosos do mundo real para download de arquivos,e-mail eataquesde aplicações webenquantotestaoscontrolesde segurançadarede. 3.9.8.27.7. Asameaçascontidasnobancodedadosdetratamentodevemserreferenciadasde

acordocomoseguinteconjuntodeinformações,incluindo,masnãoselimitandoa:

• Númerodeidentificaçãoexclusivodaameaça(uniqueID)

• Datadelançamentodaameaça

• Umadescriçãobaseadaemtextodaameaça

• Agravidadedaameaçaestádeacordocomaseguinteescala:Baixa,Médio,Alto.

• PlataformasAfetadas,

• Setoralvo,

• Regiãosegmentada

• Objetivosdoatacante,

• Ações,

• Cargasúteis,linhasdecomandodeprocessoexecutadasouvaloresdehashcombaseem tipo de ataque,

• Referênciasembancosdedadosconhecidospublicamente:virustotal

• Referênciasnasseguintesclassificaçõesdeameaçasreconhecidaspelosetore

• sistemasdeenumeração:CVE,CWE,CVSS,OWASP.

• Sistemasoperacionaisafetadospelaameaça

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

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

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.

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

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

A solução deve realizar testes SMTP da internet para o domínio corporativo.3.9.8.29.2. A solução deve realizar ataques deURL usando o protocolo SMTP da internet para o

domíniocorporativo(e-mail).

3.9.8.29.3. Asoluçãodevesuportarumsimuladordee-mailsemagenteparatestesdeataquepor e-mail.

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

AsoluçãodeveexecutarataquesdeaplicaçõesWebemHTTPeHTTPS.

Obancodedadosdeataquesdasoluçãodeveincluirpelomenos169(centoesessenta e nove) assinaturas exclusivas de ataques de aplicações web na biblioteca de ameaças.

Asoluçãodeveusaropayloadrealdaameaçaparaavaliaçãodocontroledesegurança, em vez de usar a "reprodução de PCAP" para ataques a aplicações web.

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

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.

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

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

AsoluçãodevesercapazdevalidarsoluçõesDLPdeendpoint,emailerede.

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

AsoluçãodeveabrangertécnicasdeexfiltraçãopelomenosnosprotocolosHTTP,HTTPS e TCP.

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

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

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.

Asoluçãodevepermitirqueosusuárioscriemataquespersonalizadosdeinfiltraçãode rede(downloaddearquivo)usandoumabibliotecadeameaçasexistentecompelomenos

8.000(oitomil)arquivosmaliciososdisponíveis.

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.

Asoluçãodevepermitirqueosusuárioscriemataquesdee-mailpersonalizadosusando a biblioteca de ameaças existente com pelo menos 7400 (sete mil e quatrocentos) arquivos maliciosos disponíveis.

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.

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.

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

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.

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.

A solução deve apresentar e classificar assinaturas e mitigações por gravidade e categoria (ataquesde aplicaçõesweb, exploração de vulnerabilidades, códigosmaliciosos) das ameaças relacionadas.

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

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

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

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

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.

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.

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(funcionalidadedeprevençãodeintrusãoderede)

• Fortigate(prevençãodeintrusãoderedeeaplicaçãoweb)

• McAfee/Trellix(funcionalidadedeprevençãodeinvasõesderede)

• ModSecurity(OpenSource)(firewalldeaplicativodaweb)

• Snort(códigoaberto)(prevençãodeintrusãoderede)

• TrendMicro(prevençãodeinvasãoderede)

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

A solução deve executar ataques cibernéticos sem implantar serviços vulneráveis. 3.9.8.35.2. Asolução deveavaliaroscontrolesEndpoint, Network eEmailSecurity executadosem

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 .

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.

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).

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.

Apropostadesoluçãodevepermitiraconfiguraçãodecadaagenteparaquesugestões de mitigação possam ser geradas de acordo com uma lista de tecnologias de fornecedores.

Asoluçãodeveterpelomenosmedidasdecomunicaçãoeautenticaçãocriptografadas baseadasemcertificadoparaprotegeras comunicaçõesentreseuscomponentesdesoftware.

Asoluçãoaserutilizadanaprestaçãodestesserviçosdeveatendera,nomínimo,asServiçosde Detecção e Analytics:

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)).

Aoseconectaràssoluções SIEMeEDR,asoluçãodevefornecer umaconexãovia "API" usando autenticação de usuário-senha ou token.

Apósaconfiguraçãodasoluçãoparaintegraçãocomsoluções SIEMouEDR,eladeverá ser capaz de emitir um aviso em caso de problemas de acesso.

Aoconfiguraraconectividadecomsoluçõesdelogrelevantesparaevitarfalhasevalidar osdadosdelog,asoluçãodeveterumafuncionalidadededicadaparatestarautomaticamente a precisão e a operação correta das consultas definidas pelo usuário.

Asolução devefornecer uma interface para determinar quandoasconsultas são feitas após o término dos ataques. (Tempo de atraso)

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)

Asolução deve forneceruma interface para definirumlimitedeconsultas simultâneas que podem ser feitas à solução SIEM/EDR para realizar análises de detecção de ameaças paralelas ao mesmo tempo.

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.

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.

Asoluçãodeveoferecersuporteaosresultadosdaanálisededetecçãoaseremexibidos de acordo com as categorias de ataque (Download de arquivo, Aplicações Web e Ataques de cenário de endpoint do Windows).

Asolução deveforneceruma interfacepara visualizar ecomparar ostatusdedetecção nos últimos 7/30/90 dias.

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

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".

A solução deve ser capaz de produzir no formato CSV com a finalidade de relatar ameaçasdetectadasounãodetectadasedevesercapazdemostrarseumalarmefoidisparado após um ataque simulado ou não.

A solução deveser capaz degerar resultadosdedetecção deameaçasemumrelatório PDF com ameaças registradas ou não registradas e ameaças alertadas ou não alertadas.

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

Osresultadosdealertaparaosataquesdecenáriodeendpointdevemser combinados com as técnicas e táticas da estrutura MITRE ATT&CK pela solução.

A solução deve validar os eventos ou logs recolhidos dos sistemas com os quais está integrada(nomeadamentesoluções LogManagement,SIEMouEDR)paramostraraqueles

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

Asoluçãodevesercapazdepermitirqueosusuáriosselecionemsedesejamarmazenar a saída bruta do log de detecção das fontes de dados.

Deveserpossíveldefiniroarmazenamentodelogs.

Deveser possíveldefiniro número deentradasdelogsregistradasemcada simulação. 3.9.8.36.22. Asoluçãoaserutilizadanaprestaçãodestesserviços deve atendera,nomínimo,as

seguintesfuncionalidadesdeRelatoria:

Asoluçãodeverelataronúmerototaldesimulaçõesdeataqueexecutadas,juntamente com o número de ataques bloqueados e não bloqueados, para cada simulação. Uma lista de ataques totais bloqueados e não bloqueados será fornecida.

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).

Asoluçãodeveforneceruma interfacegráficaparacompararasmudançasdestatusde segurança nos últimos 07/30/90 dias.

Asoluçãodevepermitirageraçãoderelatóriosindividuaisdesimulaçãoparaprevenção e detecção ou apenas para resultados de prevenção nos formatos CSV e PDF sob demanda.

SERVIÇOSDECONTROLEEAUDITORIADEACESSOS

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.

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.

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:

Suportar o acesso externo a rede semqualquer necessidadedeutilização deVPN ou método similar de acesso;

Permitiroacessoremoto,nomínimo,aosseguintessistemasoperacionais:

MicrosoftWindows10esuperiores;

ServidoresWindowsServer2012esuperiores;

LinuxRedHatEnterprise6.0esuperiores.

UtilizarprotocolosdecomunicaçãofazendousodecriptografiaTLS1.2ousuperior;

Suportarofuncionamentoaredesquenãoestãoconectadasdiretamenteainternetearedes seguras;

Suportaroacessosemnecessidadedepermissãopréviaparaoacessoadesktopseservidores;

PossibilitaroacessoadispositivosderedeviaSSH,comoroteadoreseswitches;

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

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;

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);

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

Permitirforçaroencerramentodasessãoremotapelosupervisor,comnotificaçãoaocliente;

Provermonitoramentoaovivoegravaçãodasessão,comregistrocompletodasatividades executadas durante a sessão executada pelos usuários;

Limitar o acesso a aplicativosespecificados no sistema remoto, incluindo a acesso a área detrabalho remota;

SuportarfiltrodecomandosduranteassessõesSSH,visandoevitarqueousuário inadvertidamente use um comando que pode causar danos ao servidor acessado;

SuportarainjeçãoautomáticadecredenciaisemsistemasWindows,permitindoqueosusuários autentiquem ou elevem privilégios sem revelar credenciais, bem como a ação de “executar como”;

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;

Suportaroacessocomosseguintesmodos: 3.9.9.20.1. Através de clientes instalados;

Atravésdeagentedeproxylocal,quepermiteoacessoasistemasautônomosemuma rede, sem cliente pré-instalado;

Acessoviaagentedeproxylocal,quepermiteoacessoasistemasemumarederemota que não tenha uma conexão de internet nativa;

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

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

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;

Permitirqueosusuáriostransfiramarquivosdamáquinaemqueestáconectadoparaosistema remoto, através da console da solução e sem necessidade de uso de ferramentas de terceiros;

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;

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

Asoluçãodevepossuirintegraçãocomsoluçõesde ITSM

Asoluçãodeveproverautenticaçãoviakerberos

REQUISITOSDEEQUIPEECAPACITAÇÃOTÉCNICADEANALISTASLOCADOSPARAPRODEB

Deverá conter no mínimo 2 (dois) profissionais que serão considerados como prepostos da CONTRATADA,comperfildeAnalistadeSegurança,sendo1(um)comperfildeAnalistadeSegurança 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).

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

Deverãotergraduaçãoemcursosdetecnologiadainformação,engenhariadecomputaçãoe/ou pós-graduação em segurança da informação;

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

Aequipedeverápossuir,somados,nomínimo,3(três)dascertificaçõestécnicasabaixolistadas: 3.9.10.5.1. Certified Information Security Manager (CISM).

3.9.10.5.2. CertifiedInformationSystemsSecurityProfessional(CISSP). 3.9.10.5.3. EC-Council Certified Ethical Hacker Master.

3.9.10.5.4. EC-CouncilCertifiedEthicalHackerPractical. 3.9.10.5.5. CompTIA Security +.

CompTIACySA+.

CompTIACASP+.

EC-Council Certified SOC Analyst (CSA). 3.9.10.5.9. EC-CouncilCertifiedIncidentHandler(E|CIH). 3.9.10.5.10. GIAC Certified Incident Handler (GCIH).

3.9.10.5.11. GIACContinuousMonitoringCertification(GMON). 3.9.10.5.12. EXIN ISFS Foundation.

LinuxProfessionalLPIC.

Vulnerability Management Foundation. 3.9.10.5.15. ISO/IEC27001:2013Foundation(I27001F).

3.9.10.5.16. ICSI|CertifiedNetworkSecuritySpecialist(CNSS). 3.9.10.5.17. Scrum Foundation Professional Certificate 3.9.10.5.18. ITIL Foundation

COBITFoundation

CompTIA Advanced Security Practitioner (CASP+) 3.9.10.5.21. CybersecurityProfessionalCertificate–LCSPCbyCyBok.

REQUISITOSDEEQUIPEECAPACITAÇÃOTÉCNICADEANALISTASREMOTOS

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.

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.

OconjuntodaequipealocadapelaCONTRATADAdeverácomprovarascertificaçõestécnicasdos fabricantes de todas as soluçõesconstante no ANEXO III – SOLUÇÕES DE SEGURANÇA além das certificações conforme requisito constante no item 5.9.10.5;

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

INDICADORESDEPERFORMANCE

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 oquintodiaútil domês subsequente ao da prestação do serviço.

Devemconstardesserelatório, 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.

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;

ITEM10-SERVIÇOSPROFISSIONAISDEMONITORAMENTOESEGURANÇAPARAOITEM“SOLUÇÃODE SEGURANÇA DE ENDPOINT - EPP” PARA CADA ITEM MONITORADO PELO PERÍODO DE 24 MESES

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 EndpointProtectionespecificadanoitem“ServiçosProfissionaisdeMonitoramentoeSegurançaparaoitem “Solução de Segurança de Endpoint - EPP” para cada item monitorado pelo período de 24 Meses.” deste Termo de Referência, conforme as necessidades da CONTRATANTE;

O serviço deverá ser iniciado após a emissão da Ordem de Serviço, a ser enviada pela CONTRATANTE,apósaentregadoTermodeHomologaçãodeinstalação doitem“ServiçosProfissionaisdeMonitoramento eSegurançaparaoitem“SoluçãodeSegurançadeEndpoint-EPP”paracadaitemmonitoradopeloperíodo de 24 Meses.”;

Os serviços serão pagos mensalmente, de acordo com o volume de dispositivosa serem monitoradospela CONTRATADA.

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

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;

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;

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;

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

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;

A documentação deverá ser aprovada pela CONTRATANTE e pelo GESTOR TÉCNICO, caracterizando a homologação da solução em umprazo de até10 diasúteis, quandoa CONTRATANTE emitirá umTermode Homologação;

Caso seja identificado defeito ou falha sistemática em determinado produto/serviço entregue pela CONTRATADA,ouainda,quenostestesrealizadossejamconsideradosemdesacordocomasespecificações

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

ACONTRATADAseráresponsávelpelomonitoramentodasoluçãoemregime24x7x365,devendomanter a mesma sempre atualizada e em operação;

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 conformidadeoperacionaldo ambiente. Aformataçãodesterelatório deveestar emcomumacordocoma CONTRATANTE;

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:

Desinstalação,reconfiguraçãooureinstalaçãodecorrentesdefalhasnosoftware,atualizaçãoda versãodesoftware,correçãodedefeitos,ajustesereparosnecessários,deacordocomosmanuaise as normas técnicas específicas para os recursos utilizados;

Quantoàsatualizaçõespertinentesaossoftwares,entende-secomo“atualização”oprovimento detodaequalquerevoluçãodesoftware,incluindocorreções,patches,fixes,updates,servicepacks, novasreleases,versions,builds,upgrades,englobandoinclusiveversõesnãosucessivas,noscasosem que a liberação de tais versões ocorra durante o período de garantia especificado;

A CONTRATADA deverá monitorar índice de atualização do conteúdo de segurança (ex: assinaturas) e engines/motoresdedetecçãoalertandoquandoíndicedeatualizaçõesdasmáquinasestiverabaixode90%;

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;

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

No caso de necessidade de ações preventivas ou corretivas a CONTRATADA agendará com antecedência juntoaCONTRATANTEasimplementaçõesdascorreções,foradohoráriocomercial,preferencialmenteem feriadosefinaisdesemana.Nenhumaaçãopoderáserexecutadanoambientesemaciênciaeanuênciado CONTRATANTE;

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

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;

Os acionamentos dos serviços de suporte e manutenção serão requisitados por meio de ordens deserviço,aseremabertaspeloCONTRATANTE,através denúmerodetelefonenacional(0800comserviçode uso ilimitado) disponibilizado pela CONTRATADA, e ainda, por e-mail e sítio de internet;

Nãohaverálimitaçãononúmerodechamadosquepoderãoserabertos;

ACONTRATADAmanteráregistrodetodasasordensdeserviçoabertas,disponibilizando,paracadauma,no mínimo as seguintes informações:

Númerosequencialdaordem;

Dataehoradeabertura;

Severidade;

Descriçãodoproblema;

Dataehoradoinício doatendimento;

Dataehoradetérminodoatendimento(solução).

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

AsinformaçõesrelacionadasàANSestãonaSeção–AcordodeNíveldeServiço–ANS.

ITEM11 - 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.

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.

O serviço deverá ser iniciado apósa emissão da Ordem de Serviço, a ser enviada pela CONTRATANTE,apósaentregadoTermodeHomologaçãodeinstalaçãodoitem“SERVIÇOSPROFISSIONAISDE

MONITORAMENTOESEGURANÇAPARAOITEM“SOLUÇÃOPARADUPLOFATORDEAUTENTICAÇÃO-TOKEN MOBILE” PARA CADA ITEM MONITORADO PELO PERÍODO DE 24 MESES”;

Os serviços serão pagos mensalmente, de acordo com o volume de dispositivosa serem monitoradospela CONTRATADA.

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

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;

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;

O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem comomateriaiscomplementaresestritamentenecessáriosàinstalação ouàassistênciatécnicaédeinteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;

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

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;

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;

A documentação deverá ser aprovada pela CONTRATANTE e pelo GESTOR TÉCNICO, caracterizando a homologação da solução em umprazo de até10 diasúteis, quandoa CONTRATANTE emitirá umTermode Homologação;

Caso seja identificado defeito ou falha sistemática em determinado produto/serviço entregue pela CONTRATADA,ouainda,quenostestesrealizadossejamconsideradosemdesacordocomasespecificações técnicas requeridas, o Gestor Técnico e a CONTRATANTE podem exigir a substituição, total ou parcial, do referido produto;

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 conformidadeoperacionaldo ambiente. Aformataçãodesterelatório deveestar emcomumacordocoma CONTRATANTE;

Amanutençãovisamanteremperfeitoestadodeoperaçãoosserviçosfornecidosematendimentoao

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

No caso de necessidade de ações preventivas ou corretivas a CONTRATADA agendará com antecedência juntoaCONTRATANTEasimplementaçõesdascorreções,foradohoráriocomercial,preferencialmenteem feriadosefinaisdesemana.Nenhumaaçãopoderáserexecutadanoambientesemaciênciaeanuênciado CONTRATANTE;

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

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;

Os acionamentos dos serviços de suporte e manutenção serão requisitados por meio de ordens deserviço,aseremabertaspeloCONTRATANTE,através denúmerodetelefonenacional(0800comserviçode uso ilimitado) disponibilizado pela CONTRATADA, e ainda, por e-mail e sítio de internet;

Nãohaverálimitaçãononúmerodechamadosquepoderãoserabertos;

ACONTRATADAmanteráregistrodetodasasordensdeserviçoabertas,disponibilizando,paracadauma,no mínimo as seguintes informações:

Númerosequencialdaordem;

Dataehoradeabertura;

Severidade;

Descriçãodoproblema;

Dataehoradoiníciodoatendimento;

Dataehoradetérminodoatendimento(solução).

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

AsinformaçõesrelacionadasàANSestãonaSeção–AcordodeNíveldeServiço–ANS.

ITEM12-SERVIÇOSPROFISSIONAISDEMONITORAMENTOESEGURANÇAPARAOSITENS“SOLUÇÃODE SEGURANÇA DE REDE NGFW TIPO I, II” PARA CADA ITEM MONITORADO PELO PERÍODO DE 24 MESES.

A CONTRATADA deverá prestar serviços de configuração, administração, operação, atendimento a mudanças e requisições, aplicação de melhores práticas do fabricante, monitoramento e resposta a incidentesparaasoluçãodengfwespecificadanositens“soluçãodesegurançaderedengfwtipoi,ii”deste Termo de Referência, conforme as necessidades da CONTRATANTE.

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;

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

AUNIDADEdecontratação paraprestaçãodestesserviçosmensaisaplica-seacadaunidadededispositivo a ser monitorado pela CONTRATADA.

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

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;

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;

O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem comomateriaiscomplementaresestritamentenecessáriosàinstalaçãoou àassistênciatécnicaédeinteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;

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

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;

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;

A documentação deverá ser aprovada pela CONTRATANTE e pelo GESTOR TÉCNICO, caracterizando a homologaçãodasoluçãoemumprazodeaté10(dez)diasúteis,quandoaCONTRATANTEemitiráumTermo de Homologação;

Caso seja identificado defeito ou falha sistemática em determinado produto/serviço entregue pela CONTRATADA,ouainda,quenostestesrealizadossejamconsideradosemdesacordocomasespecificações técnicas requeridas, o Gestor Técnico e a CONTRATANTE podem exigir a substituição, total ou parcial, do referido produto;

ACONTRATADAserásresponsávelpelomonitoramentodasoluçãoemregime24x7x365,devendomanter a mesma sempre atualizada e em operação;

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 conformidadeoperacionaldo ambiente. Aformataçãodesterelatório deveestar emcomumacordocoma CONTRATANTE;

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:

Desinstalação, reconfiguração ou reinstalação decorrentes defalhasno software, atualização da versãode software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

Quanto às atualizações pertinentes aos softwares, entende-se como “atualização” o provimento de toda e qualquer evolução desoftware, incluindo correções, patches, fixes, updates, servicepacks, novasreleases,

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

Aoperaçãoeadministração(gerenciamentototal)dasoluçãoserárealizadapelaCONTRATADAconformeas orientações e solicitações de configurações e políticas realizadas pelo Gestor Técnico da CONTRATANTE;

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

No caso de necessidade de ações preventivas ou corretivas a CONTRATADA agendará com antecedência juntoaCONTRATANTEasimplementaçõesdascorreções,foradohoráriocomercial,preferencialmenteem feriadosefinaisdesemana.Nenhumaaçãopoderáserexecutadanoambientesemaciênciaeanuênciado CONTRATANTE;

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

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;

Os acionamentos dos serviços de suporte e manutenção serão requisitados por meio de ordens deserviço,aseremabertaspeloCONTRATANTE,através denúmerodetelefonenacional(0800comserviçode uso ilimitado) disponibilizado pela CONTRATADA, e ainda, por e-mail e sítio de internet;

Nãohaverálimitaçãononúmerodechamadosquepoderãoserabertos;

ACONTRATADAmanteráregistrodetodasasordensdeserviçoabertas,disponibilizando,paracadauma,no mínimo as seguintes informações:

Númerosequencialdaordem;

Dataehoradeabertura;

Severidade;

Descriçãodoproblema;

Dataehoradoiníciodoatendimento;

Dataehoradetérminodoatendimento(solução).

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

AsinformaçõesrelacionadasàANSestãonaSeção–AcordodeNíveldeServiço–ANS.

ITEM13-SERVIÇOSPROFISSIONAISDEMONITORAMENTOESEGURANÇAPARAOITEM"SOLUÇÃODE SEGURANÇA DE APLICAÇÕES WAF TIPO I" PARA CADA ITEM MONITORADO PELO PERÍODO DE 24 MESES.

A CONTRATADA deverá prestar serviços de configuração, administração, operação, atendimento a mudanças e requisições, aplicação de melhores práticas do fabricante, monitoramento e resposta a incidentesparaasoluçãodeWAF(WebApplicationFiewall)especificadanoitem"SOLUÇÃODESEGURANÇA DE APLICAÇÕES WAF TIPO I" deste Termo de Referência, conforme as necessidades da CONTRATANTE.

O serviço deverá ser iniciado após a emissão da Ordem de Serviço, a ser enviada pela CONTRATANTE,apósaentregadoTermodeHomologaçãodeinstalaçãodoitem"SOLUÇÃODESEGURANÇADEAPLICAÇÕES WAF TIPO I";

Osserviçosserãopagosmensalmente,deacordocomo volumededispositivosa serem monitoradospela CONTRATADA.

AUNIDADEdecontrataçãoparaprestaçãodestesserviçosmensaisaplica-seacadadispositivoaser monitorado pela CONTRATADA.

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

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;

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;

O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem comomateriaiscomplementaresestritamentenecessáriosàinstalaçãoouàassistênciatécnicaédeinteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;

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

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;

A documentação deverá ser aprovada pela CONTRATANTE e pelo GESTOR TÉCNICO, caracterizando a homologação da solução em umprazo de até10 dias úteis, quando a CONTRATANTE emitirá umTermo de Homologação;

Caso seja identificado defeito ou falha sistemática em determinado produto/serviço entregue pela CONTRATADA,ouainda,quenostestesrealizadossejamconsideradosemdesacordocomasespecificações técnicas requeridas, o Gestor Técnico e a CONTRATANTE podem exigir a substituição, total ou parcial, do referido produto;

ACONTRATADAseráresponsávelpelomonitoramentoda soluçãoemregime24x7x365,devendomanter a mesma sempre atualizada e em operação;

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 conformidadeoperacionaldo ambiente. Aformataçãodesterelatório deveestar emcomumacordocoma CONTRATANTE;

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:

Desinstalação, reconfiguração ou reinstalação decorrentes defalhasno software, atualização da versãode software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

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

Aoperaçãoeadministração(gerenciamentototal)dasoluçãoserárealizadapelaCONTRATADAconformeas orientações e solicitações de configurações e políticas realizadas pelo Gestor Técnico da CONTRATANTE;

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

No caso de necessidade de ações preventivas ou corretivas a CONTRATADA agendará com antecedência juntoaCONTRATANTEasimplementaçõesdascorreções,foradohoráriocomercial,preferencialmenteem feriadosefinaisdesemana.Nenhumaaçãopoderáser executadanoambientesemaciênciaeanuênciado CONTRATANTE;

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

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;

Os acionamentos dos serviços de suporte e manutenção serão requisitados por meio de ordens deserviço,aseremabertaspeloCONTRATANTE,através0denúmerodetelefonenacional(0800comserviçode uso ilimitado) disponibilizado pela CONTRATADA, e ainda, por e-mail e sítio de internet;

Nãohaverálimitaçãononúmerodechamadosquepoderãoserabertos;

ACONTRATADAmanteráregistrodetodasasordensdeserviçoabertas,disponibilizando,paracadauma,no mínimo as seguintes informações:

Númerosequencialdaordem;

Dataehoradeabertura;

Severidade;

Descriçãodoproblema;

Dataehoradoiníciodoatendimento;

Dataehoradetérminodoatendimento(solução).

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

AsinformaçõesrelacionadasàANSestãonaSeção–AcordodeNíveldeServiço–ANS.

4. DAINSTALAÇÃOEHOMOLOGAÇÃO:

INSTALAÇÃOEHOMOLOGAÇÃODOSITENS01,02,03,04,05

Ematé10 (dez) diasúteisapósa 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;

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;

Duranteainstalação,osprofissionaisdaCONTRATADAdeverãoinformartodasasaçõesexecutadasparaos profissionais indicados pela CONTRATANTE;

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

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

Deverão ser fornecidos pela CONTRATADA, quanto a instalação física, todos os cabos e conectores necessários,refefernetesaositens01a 08,bemcomoosparafusos,porcas-gaiola,organizadoresedemais acessórios necessários para montagem apropriada dos equipamentos no rack da CONTRATANTE;

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;

Após a assinatura do instrumento contratual e até a entrega dos equipamentos, serão realizadas reuniões preparatórias,remotasoupresenciais,casonecessários,comapresençadosintegrantesdaequipetécnica daCONTRATADA,daqualselavraráataparapermitiroacompanhamentocriteriosodaexecuçãodoobjeto;

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

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

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

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;

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;

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

Adocumentaçãodeveráserentregueemmeiodigital(formatosPDFeDOCx);

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

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

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;

Durante a etapa de homologação, caso a equipe técnica da CONTRATANTE identifique inconformidadena 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;

Não haverá custos adicionais à CONTRATANTE para a realização das correções apontadas, sendonecessária 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;

SãocondiçõesparaaassinaturadoTermodeHomologaçãodoServiçoporpartedaCONTRATANTE:

ACONTRATANTEreceberocomunicadodaCONTRATADAinformandodaconclusãodosserviços de instalação, conforme descrito neste Termo de Referência;

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

ACONTRATANTErecebertodadocumentaçãoatualizadaquecontempla:

Visãogeraldaarquiteturadasoluçãoimplantada,comdesenhodaestruturalógicaefísica adotada quando necessário;

Descriçãodasetapasdoprocessodeinstalação,detalhandoasopçõesdeconfiguraçãoadotadas;

Descriçãodofuncionamentodassoluções,incluindomanuaisdeutilizaçãodosportaiswebpara visibilidade, para procedimento de abertura de chamado junto a CONTRATADA.

INSTALAÇÃOEHOMOLOGAÇÃODOSITENS06,07,08noDATACENTERdaPRODEB

ACONTRATADAematé10(dez)úteisdiasapósaassinaturadocontrato,deveráiniciaroplanejamentopara elaboraçãodoCronogramadeInstalaçãodosequipamentosesoluções,emconjuntocomaCONTRATANTE;

Duranteainstalação,osprofissionaisdaCONTRATADAdeverãoinformartodasasaçõesexecutadasparaos profissionais indicados pela CONTRATANTE;

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;

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;

Será apresentado pela CONTRATADA Projeto Executivo: Elaboração de projeto prévio para a implantação da solução conforme parâmetros do Termo de Referência.

OPlanodeInstalaçãodasoluçãopoderáserrecusadopelaCONTRATANTE,devendoaCONTRATADArealizar os ajustes definidos em reunião e reapresentá-los;

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;

Concluídooserviçodeinstalaçãoeostestes,a CONTRATADAdeverá elaboraradocumentaçãodasolução, contendotodasasinformaçõesdaimplantação,comoaspectosdearquitetura,configuração,descriçãodas características e recursos utilizados, testes, integrações e etc.;

Adocumentaçãodeverá seremitidacomtimbredaCONTRATADAedeveráconternome,dataeassinatura do técnico responsável da CONTRATADA;

Adocumentaçãodeveráserentregueememmeiodigital(formatosPDFeDOCx);

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

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;

Durante a etapa de homologação, caso a equipe técnica da CONTRATANTE identifique inconformidadena implantação da solução instalada, é de responsabilidade da CONTRATADA, iniciar as devidas correçõesnum prazo de 3 (três) dias úteis após a emissão do relatório de inconformidade;

Não haverá custos adicionais à CONTRATANTE para a realização das correções apontadas, sendonecessária 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;

SãocondiçõesparaaassinaturadoTermodeHomologaçãodoServiçoporpartedaCONTRATANTE:

ACONTRATANTEreceberocomunicadodaCONTRATADAinformandodaconclusãodosserviços de instalação, conforme descrito neste Termo de Referência;

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

ACONTRATANTErecebertodadocumentaçãoatualizadaquecontempla:

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

Descriçãodasetapasdoprocessodeinstalação,detalhandoasopçõesdeconfiguraçãoadotadas;

Descriçãodofuncionamentodassoluções,incluindomanuaisdeutilizaçãodosportaiswebpara visibilidade, para procedimento de abertura de chamado junto a CONTRATADA.

IMPLANTAÇÃOEHOMOLOGAÇÃODOSSERVIÇOSDOITEM09

Ematé 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;

No prazo de até 30 (trinta) dias após a emissão da Ordem de Serviço, a CONTRATADA deverá realizar avaliaçãocompletadoambientedoCONTRATANTEcomoobjetivoidentificarlacunasouoportunidadesde melhoria (Gap Analysis) com o objetivo de avaliar a maturidade dos controles de segurança do CONTRATANTE;

A CONTRATADA deverá realizar toda a instalação dos produtos que forem necessários, incluindo a configuração:dosprodutosinstalados,dossensoresoucoletores,esenecessário,ajustesnainfraestrutura, e os testes da solução, sob supervisão da CONTRATANTE;

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.

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.

Os softwares ofertados devem estar licenciados pela CONTRATADA, ser instalados em sua versão mais estáveleatualizadaeestarcobertosporcontratosdesuporteeatualizaçãodeversãodofabricantedurante a vigência do respectivo item de serviço.

Os equipamentos e softwares não podem constar, no Plano de Implantação, em listas de end-of-lifesale, end-of-support,end-of-lifeousimilaresdofabricante,ouseja,nãopodemterprevisãodedescontinuidade de fornecimento, suporte ou vida;

Todainstalaçãoeconfiguraçõesdeverãoseracompanhadaspelaequipetécnicada CONTRATANTE;

ACONTRATADAserárespons ável por dimensionara soluçãoaseradotadanarede daCONTRATANTE.Esta solução estará sujeita à análise e aprovação da equipe técnica da CONTRATANTE;

A solução apresentada não pode causar impacto no funcionamento da rede (por exemplo, lentidão narede local, degradação no desempenho das estações de trabalho e servidores, entre outros), devendo ser transparente;

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 alíneaanterior,asoluçãodeveráserredimensionada,incluindoadição/substituiçãodehardware,software, licenças, etc, providos pela CONTRATADA sem ônus adicional para a CONTRATANTE;

Todos os técnicos envolvidos na implantação e configuração devem possuir conhecimentos técnicos aprofundados nos produtos que ficarem sob sua responsabilidade;

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;

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;

A CONTRATADA com auxílio da CONTRATANTE irá preparar um Plano de Testes onde devem estardescritos 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;

O Plano de Testes deve ser apresentado em forma de tabela a fim de facilitar o acompanhamento dos mesmos por parte da CONTRATANTE;

Na tabela mencionada na alínea anterior, deve-se incluir os resultados esperados para cada testerealizado;

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;

Caso seja detectado qualquer problema nos testes, em qualquer uma das funcionalidades, a CONTRATADAdeveráefetuar asdevidascorreçõese,apósarealizaçãodessascorreções, ostestesserão reiniciados;

Se todos os testes forem realizados com sucesso, a solução será considerada implantado, num prazo de 2 (dois)diasúteis, dar-se-áinícioao PeríododeFuncionamentoExperimental -PFE,comduraçãode10(dez) dias úteis, para homologação da solução

O PFE - Período de Funcionamento Experimental é estabelecido pela CONTRATANTE para testar o perfeito funcionamentodasolução,verificarsuasfuncionalidades,analisandosuaaderênciaàsespecificaçõesdeste

EditaleseusAnexos,bemcomoàPropostadaCONTRATADA,easuacompatibilidadecomaestrutura operacional já existente na CONTRATANTE;

Durante o PFE, não deve ocorrer qualquer falha ou interrupção em qualquer uma das funcionalidades da solução fornecida;

A aprovação da solução será vinculada também à entrega da Documentação Técnica– DT e integração com a ferramenta ITSM da CONTRATANTE;

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.

Caso não haja qualquer falha ou interrupção novamente em qualquer uma das funcionalidades, a solução será considerada homologada.

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.

Ematé10diasúteisapósafinalizaçãodoPFE,aCONTRATADAapresentaráumrelatóriocomalinhabasede funcionamentonormal,baseadonasrecomendaçõesdofabricante,paracadaumdosprodutos 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;

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;

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.

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

EQUIPAMENTOSELICENÇAS DOSITENS01,02,03,04,05,06,07e08

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;

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;

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;

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;

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. LOCALPARAENTREGA

PARAOSITENS01,02,03,04 e05

AsentregasdeverãoserrealizadaspelaCONTRATADAnasededaCONTRATANTEsituadanaRegião Metropolitana de Salvador;

Asentregasdeverãoserrealizadasemdiasúteis,obedecendoaoshoráriosabaixodiscriminados:

Segundaaquinta:08:00hsàs12:00hsedas13:30hsàs17:30hs;

Sexta:08:00hsàs12:00hsedas13:30hsàs16:00hs.

PARAOSITENS06,07e08

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;

Asentregasdeverãoserrealizadasemdiasúteis,obedecendoaoshoráriosabaixodiscriminados:

Segundaaquinta:08:00hsàs12:00hsedas13:30hsàs17:30hs;

Sexta:08:00hsàs12:00hsedas13:30hsàs16:00hs.

7. GARANTIAELICENCIAMENTODOSITENS01a 08

No momento da entrega do hardwareesoftwarea CONTRATADA deverá apresentar termo degarantia 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;

Aofimdocontratodegarantia elicenciamento, a solução deverá semanterfuncional, capaz decriar,customizar egerenciar políticaseregras, gerar e encaminhar logs, manipular dashboard eentre outrasfunçõesnecessárias ao manuseio da solução, exceto para funcionalidades que dependam de serviços hospedados em nuvem;

Paraoacompanhamentodagarantia,aCONTRATADAdeverádisponibilizarprofissionaisespecializadoscomo objetivo de manter em perfeito estado de operação os serviços e equipamentos;

Para a garantia técnica, a CONTRATADA deverá observar os procedimentos destinados a recolocar 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,fornecimentodepeçasdereposição,substituiçãodehardware,atualizaçãodaversãodedrivers, firmwaresesoftwarebásico,correçãodedefeitos,ajustesereparosnecessários,deacordocomosmanuais e as normas técnicas específicas para os recursos utilizados;

Noquetangeasoftware:desinstalação,reconfiguraçãoou reinstalaçãodecorrentesdefalhasnosoftware, 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;

Oprovimentodetodaequalquerevoluçãodesoftware,incluindocorreções,“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;

Devepermitiroacessoàbasedeconhecimentodasolução;

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;

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;

Noatendimentoaoschamadostécnicosabertos,deveráserdisponibilizadosuportepersonalizadoporanalista(s) designado(s);

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;

AprioridadedeatendimentoaoschamadosserádefinidapeloCONTRATANTE;

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;

Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços e ainda:

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,identificaçãododefeito,técnicoresponsávelpelasolução,asprovidênciasadotadaseoutras informações pertinentes. Este relatório deverá ser homologado pela CONTRATANTE, através do gestor do contrato;

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;

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 poderáserencontradonositedofabricante,através deequivalênciaesemelhança,esópoderáserefetuada mediante expressa autorização da PRODEB, para cada caso particular. Caso a PRODEB recuse o equipamento,componente,materialeoupeçaasersubstituído,olicitantedeveráapresentaralternativas, porém o prazo para solução do problema não será alterado;

Nãohaverálimitaçãononúmerodechamadosquepoderãoserabertos;

ACONTRATADAmanterá registro detodososchamadosabertos, disponibilizando, para cada um, nomínimoas seguintes informações:

Númerosequencialdaordem;

Dataehoradeabertura;

Severidade;

Descriçãodoproblema;

Dataehoradoiníciodoatendimento;

Dataehoradetérminodoatendimento(solução).

8. CRONOGRAMA

ParaosItens01a08

ATIVIDADES	PRAZO
IníciodoplanejamentoparaelaboraçãodoPlanodeInstalação, Configuração,migraçãoedemaisaçõesconjuntocomaCONTRATANTE dosItens01a 08	Até10diasapósaassinaturadocontrato
PrazodeEntregadosEquipamentos(Itens01a08)ehands-ondo produto.	Até60diasapartir daassinaturadocontrato
RecebimentoProvisóriodosEquipamentoseLicenças	Até05diasapósEntregados Equipamentos
RecebimentoDefinitivodosEquipamentostestadosemfuncionamento elicençasativadascomavalidadesolicitadanoTR	Até05(cinco)diasúteisapóso recebimento provisório
IníciodaInstalaçãodaSolução	Até15diasapósorecebimentodefinitivo
ConclusãodaInstalaçãodaSolução	Até10diasapósIníciodaInstalação da Solução
EntregadaDocumentaçãoFinal	Até10diasapósConclusãoda Instalação, Configuração
ResoluçãodeInconformidades	Até03diasapósvalidaçãoinicialda CONTRATANTE
EmissãodoTermodeHomologação	Até10diasapósentrega daDocumentaçãoFinal sem inconformidades

ParaoItem09

ATIVIDADES	PRAZO
IníciodoplanejamentoparaelaboraçãododoPlanodeImplantação emconjuntocomaCONTRATANTE	Até5(cinco)diasapósaemissãodaOrdemde Serviço
Apresentaçãodosrelatóriosdaavaliaçãodoambienteediagnóstico inicialdasvulnerabilidadesexistentesdaCONTRATANTE	Até30diasapósaemissão daOrdemde Serviço
ImplementaçãodoCentrodeOperações	Até60diasapósaemissão daOrdemde Serviço
ConclusãodaativaçãodoServiçode Monitoramento	ConformecronogramadefinidonoPlanode Implantação
IniciodaexecuçãodoPlanodeTestesparavalidaçãodasolução	5diasúteisapósaconclusãodaativação do serviço
ExecuçãodoPlanodeTestesparavalidaçãoda solução	10diasúteisapósseu início
InícidoPeríododeFuncionamentoExperimental–PFE	2diasúteisapósaconclusãodoplanode testes
FimdoPeríododeFuncionamentoExperimental–PFE	10diasúteisapósseu início

EntregadaDocumentaçãoFinaleRelatóriodeLinhaBase	Até10diasapósConclusão do FimdoPeríodode FuncionamentoExperimental– PFE
ResoluçãodeInconformidades	Até03diasapósacionamentoda CONTRATANTE
EmissãodoTermodeHomologação	Até10diasapósentrega daDocumentação Final
Emissãodaprimeiranotafiscal	30diasapósaemissão doTermode Homologação

Para os Itens 10 a 13

ATIVIDADES	PRAZO
Início do planejamento para elaboração do do Plano de Implantação em conjunto com a CONTRATANTE	Até5(cinco)diasapósaemissãodaOrdemde Serviço
ConclusãodaativaçãodoServiçodeMonitoramento	ConformecronogramadefinidonoPlanode Implantação
EntregadaDocumentaçãoFinal	Até10diasapósConclusão daAtivação
ResoluçãodeInconformidadesapósTermodeHomologação	Até03diasapósacionamentoda CONTRATANTE
EmissãodoTermodeHomologação	Até10diasapósentrega daDocumentaçãoFinal
Emissãodaprimeiranotafiscal	30diasapósaemissão doTermode Homologação

9. ACORDODENÍVELDESERVIÇO–ANSDOSITENS09a13

MétricaseConvenções

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;

PlantãoTelefônicopornúmero0800comoserviçodeusoilimitado,noperíodode24(vinteequatro) horas por dia, 07 (sete) dias por semana;

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 tambémcompreendendoosseguintestiposdeatendimentolocal:suporteparaup-gradedeversões 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.

Nãoserãoconsideradasindisponibilidadesasseguintessituações:

Janelademanutençãopreviamenteacordadaentre CONTRATANTEeCONTRATADA;

Chamadosescaladosparaofabricante,emtratamentoporeste;

IndisponibilidadedaCONTRATANTEemrealizarterefasquedependamdesta;

ParadasprogramadaspelaCONTRATADAeaprovadaspeloCONTRATANTE.Nestecaso,aautorização deve ser solicitada pela CONTRATADA com, pelo menos, 5 (cinco) dias de antecedência;

Paradasocasionadasnosequipamentosporerrosdeconfiguraçãocausadospelo CONTRATANTE,sem responsabilidade da CONTRATADA;

Paradasocasionadasporcasosfortuitosoudeforçamaior,devidamentecomprovados.

Condiçõesgeraisparatodososserviços:

Inicialmenteoatendimentopoderáserrealizadopormeio deatendimentoremotoondeaoseidentificara necessidadedeatendimentolocal(on-site),aCONTRATADAdeverádeslocarumprofissionalàunidade,para continuidade do atendimento;

Oatendimentonolocal(on-site)deveráserprovidonoambientetecnológicodaPRODEBenasUnidadesda CONTRATANTE localizadas no Estado da Bahia;

A CONTRATADA deverá responder aos acionamentos, dentro dos prazos fixados neste item, a partir da abertura do acionamento;

O término do atendimento deverá ocorrer dentro dos prazos fixados neste item, a partir do contato da equipe técnica da CONTRATADA, responsável pelo atendimento;

A abertura dos chamados deverá, sempre que possível, ser realizada a partir dos alertas registrados pela solução de monitoramento da CONTRATADA, constanto todosos detalhespara quea equipederesposta aincidentesrealizeoatendimentoconsiderandoosNíveisdeAcordodeServiçofixadosnastabelasabaixo;

A CONTRATADA deverá realizar a integração das soluções de segurança da CONTRATANTE com seu sistema de monitoramento para prover o registro dos chamados automatizados;

Emcasodeimpossibilidade,estadeveserjustificadaàCONTRATANTE,ondedeveráserelaboradoum 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;

Entende-seporiníciodoatendimentoahoradocontatodaequipetécnicadesuportedaCONTRATADAcom a equipe da CONTRATANTE;

Entende-se por término de atendimento a disponibilidade do produto para uso em perfeitas condições de funcionamento no local onde esteja instalado;

O nível de severidade e prioridade deverá ser informado pela CONTRATANTE no momento da abertura de cada chamado. A severidade e prioridade doschamadosserá definida considerando critérios de impacto e urgência conforme descrito em cada tabela abaixo;

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.

Todas as solicitações deverão ser registradas pela CONTRATADA, para acompanhamento e controle da execução dos serviços.

A CONTRATADA deverá apresentar relatório de atendimento para cada solicitação de suporte, contendo data ehora da solicitação de suportetécnico, inícioe términodoatendimento, identificaçãodoproblema, providências adotadas e demais informações pertinentes.

O relatório de atendimento deverá ser assinado pelo servidor da CONTRATANTE que solicitou o suporte técnico.

Após a conclusão do serviço é obrigação da CONTRATADA verificar o restabelecimento das condições operacionais normais;

Todo o chamado somente será caracterizado como “encerrado” mediante concordância daCONTRATANTE;

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.

Para o acompanhamento e avaliação dos serviços da CONTRATADA será estabelecido e utilizado entre as partesosNíveisMínimosdeServiço.ONMSdeveserconsideradoeentendidopelaCONTRATADAcomoum compromisso de qualidade que assumirá junto ao CONTRATANTE.

OsNMS para chamadosde incidente, requisiçõese resposta a incidentesdeverão ser baseados noslimites 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;

A CONTRATADA deverá acompanhar os Indicadores para que seja possível uma avaliação da qualidadedo serviço entregue. A partir das informações obtidas nestes indicadores será possível a aplicação do NMS (Níveis Mínimos de Serviço) no processo de pagamento.

AausênciadedadoscoletadospelaCONTRATADApoderáserconsideradaindisponibilidade.

Caso ocorra, a qualquer tempo, a não aceitação, por parte do CONTRATANTE, de quaisquer aspectos necessáriosàdeclaraçãodafatura,osprazosparaatesteserãodescontinuadosereiniciadosapósacorreção necessária. O CONTRATANTE pode, a qualquer momento, recusar-se a declarar a fatura, caso constate:

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.

Entretanto, eventuais falhas e descumprimentos contratuais verificados serão devidamente apurados em processosadministrativospróprios,podendoresultaremaplicaçãodepenalidade,semprejuízodepossível rescisão do contrato, na forma prevista na lei.

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.

NíveisMínimosdeServiçodosServiçosProfissionaisdeMonitoramentoeSegurança

NíveisMínimosdeServiçoparaatendimentoaINCIDENTESOPERACIONAIS:

Incidentesoperacionaissãoaquelesqueafetamdiretamenteassoluçõesdesegurançagerenciadase monitoradas pela CONTRATADA e consequentemente o funcionamento dos serviços do Governo do Estado que dependem delas para o seu pleno funcionamento;

OtempodoinícioefetivodeatendimentoaochamadotécnicodeveráserdeacordocomaTabelade 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 mesmonãodevendoultrapassarosprazosestabelecidosparaasrespectivasseveridades,contadosa partir da abertura do chamado técnico;

Tabeladeseveridadespara**INCIDENTES**:

Severidade	**Descrição**		
1–Crítica	Asoluçãodesegurançanãoestáoperanteenãoépossívelnenhumasolução de contorno viável. Problema na solução que gera indisponibilidade em sistemas/serviços produtivos que dependem desse ativo.		
2–Alta	Problemanasoluçãodesegurançaquegeraimpactoemdeterminadosistema/serviço produtivo que dependem desse ativo.		
3–Média	Problemacontornávelquenãogeraqualquerimpactoaossistemas/serviços produtivos que dependem desses ativos.		
4–Baixa	Consultastécnicasedúvidassobreassoluçõesdesegurança		
Severidade	**Prazodeatendimento**		
	TMIA	**TMSO**	**TMSD**
1–Crítica	15min	2h	24h
2–Alta	30min	4h	48h
3–Média	1h	8h	72h
4–Baixa	2h	16h	144h

Entende-sepor:

TMIA - Tempo máximo para início de atendimento: Tempo máximo requerido para o início do atendimento;

TMSO-Tempomáximo parasolução operacional:Tempomáximo derecuperação, ou seja, tempo requerido para contornar o problema e deixar a solução/sistema/serviço disponível;

TMSDC - Tempo máximo para solução definitiva do chamado: Tempo máximo requerido para solucionar em definitivo a causa do problema;

Um chamado somente poderá ser fechado após confirmação de responsável do CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade dorecurso para uso em perfeitascondições de funcionamento;

Este serviço deve estar disponível para acionamento e atendimento no sistema 24x7 (vinte e quatro horas por dia, sete dias na semana);

NiveisMínimosdeServiçoparaREQUISIÇÕES

Requisiçõessãotodasassolicitaçõesrealizadaspelacontratanteeporseusrespectivosusuáriose clientes para que a CONTRATADA realize determinada tarefa estabelecida no portfólio de serviços que será elaborado entre as partes;

Otempodoinícioefetivodeatendimentoaochamadotécnicodeveráserdeacordocomatabelade 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 mesmonãodevendoultrapassarosprazosestabelecidosparaasrespectivasprioridades, contadosa partir da abertura do chamado técnico;

Tabeladeprioridadespara**REQUISIÇÕES**:

Prioridade	**Descrição**
1–Crítica	Requisiçõesqueimpactamdiretamentenasegurançaeintegridadedos serviços/sistemas considerados críticos no portfolio da CONTRATANTE, ameaçamacontinuidadedosserviçosourepresentamriscosiminentes.
2–Alta	Requisiçõesquetêmumimpactosignificativo,masnãoimediatamentecrítico.Podem afetaroperaçõesimportantesouserviçosquenãosãoconsideradoscomocríticosno portfolio da CONTRATANTE.
3–Média	Requisiçõesqueafetamoperaçõesouusuáriosdeformalimitada,sem impacto imediato nos serviços essenciais.
4–Baixa	Requisiçõesquetêmbaixoimpactooperacional,geralmentetarefasdemanutenção preventive, geração de relatórios, consultas ou informações não críticas

Prioridade	**Prazodeatendimento**	
	TMIA	**TMS**
1–Crítica	15min	2h
2–Alta	30min	4h
3–Média	1h	8h
4–Baixa	2h	16h

Entende-sepor:

TMIA - Tempo máximo para início de atendimento: Tempo máximo requerido para o início do atendimento;

TMS-Tempomáximoparasolução:Tempomáximorequeridoparasolucionar arequisição;

Um chamado somente poderá ser fechado após confirmação de responsável do CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade dorecurso para uso em perfeitascondições de funcionamento;

Este serviço deve estar disponível para acionamento e atendimento no sistema 24x7 (vinte e quatro horas por dia, sete dias na semana);

NíveisMínimosdeServiçoparaatendimentoaRESPOSTAAINCIDENTESDESEGURANÇA:

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, entreoutros, ou porfalhas internasde segurança, comoerroshumanos ou falhas no sistema

Otempodoinícioefetivodeatendimentoaochamadotécnicodeveráserde acordocomatabelade 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;

Apósoiníciodoatendimento,otempodesoluçãodooperacionaledefinitivadoincidentedeveráser deacordocomastabelasabaixo,nãodevendoultrapassarosprazosestabelecidosparaasrespectivas severidades, contados a partir da abertura do chamado técnico;

Tabeladeseveridadespara**INCIDENTESDESEGURANÇA**:

Severidade	**Descrição**
1–Crítica	Incidentescomníveisderiscocríticoouvulnerabilidadesconsideradascomo críticas, identificadas pelas soluções de segurança, probabilidade de materializaçãooucommaterializaçãoconfirmadaderiscodeimpactocrítico que poderia afetar a operação da CONTRATANTE, como um ataque cibernéticoquecauseumaindisponibilidadeemqualquerserviço
2–Alta	Incidentes com níveis de risco alto ou vulnerabilidades consideradas como altas, identificadaspelassoluçõesdesegurança,probabilidadedematerializaçãooucom materializaçãoconfirmadaderiscodeimpactoaltoquepoderiaafetaraoperaçãoda CONTRATANTE, como um ataque cibernético que cause uma degradação em qualquer serviço

3–Moderada	Incidentescompossívelmaterializaçãoderiscodeimpactomoderadoou 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,esclarecimentostécnicosrelativosaousoeaprimoramentodosserviços contratados ou equipamentos fornecidos		
Severidade	**Prazodeatendimento**		
	TMIR	**TMCI**	**TMR**
1–Crítica	15min	2h	24h
2–Alta	30min	4h	48h
3–Média	1h	8h	72h
4–Baixa	2h	16h	144h

Entende-sepor:

TMIR-Tempomáximoparainícioderesposta:Tempomáximorequeridoparaoinícioda resposta ao incidente de segurança;

TMCI - Tempo máximo de contenção do incidente: Tempo máximo contenção do incidente de segurança;

RMR-Tempomáximoderespostaaoincidente:Tempomáximorequeridoidentificação, contenção e mitigação ou proposição de mitigações do incidente de segurança;

Um chamado somente poderá ser fechado após confirmação de responsável do CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade dorecurso para uso em perfeitascondições de funcionamento;

Este serviço deve estar disponível para acionamento e atendimento no sistema 24x7 (vinte e quatro horas por dia, sete dias na semana);

10. DESCONTOSPORDESCUMPRIMENTODOSNÍVEISDESERVIÇODOSITENS09a 13

Nahipótese 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:

Penalidadesporcadahoracompleta que exceder os níveis de acordo	**SeveridadeIncidentes Operacionais**	**SeveridadeIncidentes de Segurança**	**Prioridadede Requisições**
0,4%	1	1	1
0,3%	2	2	2
0,2%	3	3	3
0,1%	4	4	4

Osdescontosprevistosnatabelaacimaserãocalculadostomandocomobaseovalormensaldocontratoeserão 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;

Ovalor do desconto no período será igual ao somatório das ocorrências de não atendimento ou solução nos níveis de serviço especificados;

Osdescontos aplicados só poderão ser relevados motivadamente e por conveniência administrativa, mediante ato da autoridade competente, devidamente justificado;

Casoodescontoaseraplicadosejasuperioraovalordagarantia,alémdaperdadesta,responderáocontratado pela sua diferença, ou quando for o caso, cobrada judicialmente;

Agarantiadeveráserrestabelecidaintegralmente,casotenhaincididoqualquerdescontosobreovalordesta;

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,duranteoqual,osindicadoresdeserviçonãoatingidos,terãoaplicadasasglosasconformedispostono Tópico Acordo de Níveis de Serviço, de acordo com os seguintes critérios:

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;

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;

Do61ºao90ºdia:aplicar-se-á,efetivamente,75%(setentaecincoporcento)dospercentuaisprevistosna tabela para cada ocorrência de indicadores de serviço não atingido

Após o 90º dia, aplicar-se-ão integralmente os percentuais previstos na tabela para cada ocorrência de indicadores de serviço não atingido

Casohajaprorrogaçãodevigênciacontratual,nãohaveránovoperíododeestabilização;

11. CONDIÇÕES DA ATADEREGISTRODEPREÇO

As quantidades estabelecidas para cada um dos itens são estimativas e não constituem compromisso de demanda por parte da PRODEB.

Aexistênciadepreçosregistradosnãoobrigafirmarcontratações quedelespoderãoadvir,ficando-lhefacultada a utilização de outros meios, respeitada a legislação relativa às licitações, sendo assegurada ao beneficiário do registro a preferência em igualdade de condições.

APRODEBfacultaaosÓrgãoseEntidadesdaAdministraçãoPúblicadoEstadodaBahiaaadesãoàatadeRegistro 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.

Combase 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.

ÓrgãoseEntidadesdaAdministraçãoPúblicadoEstadodaBahia,assimcomoasEmpresasPúblicaseSociedades de Economia Mista que não participaram do registro de preços, quando desejarem fazer uso da ata de registro de preços, deverão consultar a PRODEB.

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.

Competeaoórgãonãoparticipanteosatosrelativosàcobrançadocumprimentopelofornecedordasobrigações contratualmenteassumidaseaaplicação,observadaaampladefesaeocontraditório,deeventuaispenalidades decorrentesdodescumprimentodecláusulascontratuais,emrelaçãoàssuaspróprias contratações,informando as ocorrências à PRODEB.

Aata de registro de preço se destinará ao atendimento das demandas, compreendendo o territóriodo Estado da Bahia;

Oprazodevalidadedaataderegistrodepreçosseráde12(doze) meses,acontardadatadesuaassinatura.

12. CRITÉRIOS DE ACEITABILIDADE DA PROPOSTA

Nãoserãoadmitidasaspropostasquedesobedeçamaoscritériosdispostos42,IXdoRegulamentodeLicitações e Contratos da PRODEB;

AProponentedeveráreferenciarexplicitamenteemsuaproposta,aorigemdefabricaçãodo(s)equipamento(s) ofertado(s),bemcomonome(s)do(s)fabricante(s),códigosepartnumbersdetodasaspartesquecompõemos equipamentos sendo propostos de forma a deixar claro o atendimento de acordo com o exigido no edital;

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);

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;

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;

Deverãoestar inclusas no valor dos serviços, toda e qualquer despesa relativa ao deslocamento dos técnicos à instalaçãodaCONTRATANTE,bemcomoosreferentesatransporte,freteeseguro,nãoocorrendoqualquerônus adicional para a CONTRATANTE;

Aspropostas precisam conter a razão social do fornecedor, telefone para contato, preposto responsável, CNPJ, além de estarem devidamente assinadas e datadas;

Apropostadeveráteroseuprazodevalidadenãoinferiora60(sessenta)diasdasuaemissão;

Deverá ser apresentada juntamente com a proposta, uma declaração fornecida pelo fabricante dos equipamentos,empapeltimbrado,informandoquealicitanteésuarevendae/ouassistênciatécnicaautorizada, conferindo desta maneira mais segurança e confiabilidade na execução do objeto, conhecimento técnico e reposição de peças;

A exigência contida no item acima tem o objetivo de resguardar os interesses da CONTRATANTE, comprovandoaaptidãodacontratadapararealizaroserviçodesuporte,bemcomo,garantindooacessoa atualizaçõescorretivaseevolutivasdisponibilizadaspelofabricanteduranteocursodoprazodevigênciado contrato;

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;

ApropostadeveserapresentadacontendoasEspecificaçõesTécnicasaseguir:

Informaçõessobrehardwareesoftware,constando marcaemodelo,fabricanteevelocidadesdasportas;

Manuaisoudatasheetsoficiaisdo(s)fabricante(s);

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);

Anãocomprovaçãodequalquerdositensacimaimplicaránaimediatadesclassificaçãodaproponente.

13. CONDIÇÕESPARAASSINATURADOCONTRATO

Comocondiçãoparaassinaturadocontrato,aempresadeveráapresentar:

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. MODALIDADEDELICITAÇÃO

Oprocedimento 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;

Alicitação deverá ser processada eletronicamente, em razão do quanto estabelecido no art. 4º, VI, do RLC da PRODEB;

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 instaladasnaPRODEB,relacionadasnoANEXOIII,edassoluçõesdesegurançadositens1a13quesãoofertadas pela mesma. Além disso, com as soluções ofertadas pela licitante, haverá um melhor gerenciamento, monitoramento e operação, além de estarem intrinsecamente relacionados;

Ocertameadotaráomodododisputaaberto;

Nointuitodeevitarooferecimentodelances com variaçãoinsignificante,oslancesofertadosdeverãoobservar umintervalomínimodediferençadevalores,queincidirátantoemrelaçãoaoslancesintermediáriosquantoem relação à proposta que cobrir a melhor oferta, que deverá ser R$ 1.000,00 (um mil reais);

15. QUALIFICAÇÃOTÉCNICA

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;

Os atestados deverão ser impressos em papel timbrado, com nome e telefone de contato dosresponsáveis pela informação atestada, não sendo aceitas declaraçõesgenéricas de catálogos, manuais de Internet, devendo ainda atestar a satisfação com o serviço ofertado pela PROPONENTE.

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

Poderão participar do certame as pessoas jurídicas reunidas em consórcio, constituído especificamente para executaroobjetodestalicitação,limitadoatrêsparticipantes,vedadoaoconsorciadocompetirisoladamenteou atravésdemaisdeumconsórcio,devendoserobservadoodispostonoRegulamentodeLicitaçõeseContratos– RLC da PRODEB e as seguintes regras:

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) nomedoconsórcio;

b) identificaçãocompletadetodasasempresasconsorciadas,incluindoarazãosocial,CNPJeendereço;

c) indicaçãodacomposição doconsórcio,comainformaçãodopercentual/cotadeparticipaçãodecadauma 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) outorgaàempresalíderdepoderesexpressos,irretratáveiseirrevogáveis,pararepresentaroconsórcioperante 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-seaassinar,emnomedoconsórcio,quaisquerpapéisedocumentosrelacionadoscomoobjetoda licitação,firmarcontratosepraticartodososatosnecessáriosvisandoàperfeitaexecuçãodoobjetodocontrato, 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 delicitaçãoquantonadeexecuçãodoeventualcontratodeladecorrente,atéorecebimentodefinitivodoobjeto (art. 102, V do RLC da PRODEB);

g) previsão da obrigação de efetiva constituição e registro do consórcio anteriormente à celebração do contrato resultantedalicitação,nahipótesedeasconsorciadassagrarem-sevencedoras(art.102,§2o,doRLCdaPRODEB);

h) prazoestipuladoparaaduraçãodoconsórcio,quedeverácompreendertodooperíododevigênciadocontrato 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).

Aempresalíderserárespons ávelpelaapresentaçãodocredenciamento.

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).

Cadaumadasempresasconsorciadasdeveráapresentar,deformaindividualizada,mas nomesmo envelopede habilitação, a documentação exigida neste instrumento convocatório para a habilitação (art. 102, inciso III, do RLC da PRODEB).

Para efeito de qualificação técnica, considerar-se-á o somatório dos quantitativos de cada consorciado, observado, entretanto,queo consorciadoqualificadodeve serresponsávelpelaprestaçãodosserviçosa quese refira a qualificação computada na licitação (art. 102, inciso III, do RLC da PRODEB).

Asempresasconsorciadasrespondemindividualesolidariamentepelosatospraticadospeloconsórcio,tantona fasedalicitaçãoquantonadeexecuçãodocontratodeladecorrente,atéorecebimentodefinitivodoobjeto(art. 102, inciso V, do RLC da PRODEB).

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,conformeprevistonoart.212doRLC,oqualremeteaoart.185,IVdaLeiEstadualnº9.433/2005).

As empresas consorciadas não poderão alterar a constituição ou a composição do consórcio sem a prévia e expressaanuênciadoórgãocontratante,atéocumprimentodoobjetodalicitaçãocomorecebimentodefinitivo (art. 102, §4º do RLC da PRODEB).

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

Évedadaasubcontrataçãototalouparcialdoobjeto.

18. CONDIÇÕESDEPAGAMENTO

PRODEB

Opagamentoreferente aositens01 ao 08descritosneste TR,serãorealizadosem01(uma)parcela após a emissão do Termo de Homologação que caracteriza a entrega e instalação das soluções;

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;

O pagamento ocorrerá de acordo com os prazos estabelecidos no art. 10, do Regulamento de Licitaçõese Contratos da PRODEB, de acordo com o valor dos bens adquiridos, a saber:

atéR$50.000,00opagamentoseráefetuadoematé15(quinze)dias;

deR$50.000,01aR$100.000,00opagamentoseráefetuadoematé30(trinta)dias;

acimadeR$100.000,01opagamentoseráefetuadoematé45(quarentaecinco)dias;

O pagamento somente será autorizado depois de efetuado o “atesto” pela comissão ou servidor competente da CONTRATANTE na nota fiscal apresentada;

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;

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;

A CONTRATADA deverá enviar as notas fiscais e documentos relacionados ao pagamento para o e-mail: cofic.financeiro@prodeb.ba.gov.br;

Antes da realização do pagamento deverá ser comprovada pela CONTRATADA a manutenção dascondições de habilitação exigidas no edital.

ÓRGÃOSEENTIDADESDAADMINISTRAÇÃOPÚBLICADOESTADODABAHIA:

O pagamentoreferenteaositens01 ao 08descritosneste TR, serãorealizados em01 (uma)parcela após a emissão do Termo de Homologação que caracteriza a entrega e instalação das soluções;

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;

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. JUSTIFICATIVADEPREÇO

Devidoa 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.

Ovalor referencial foi obtido seguindo o rito do Art. 47 do RLC da PRODEB, sendo apurado a partir do menor valor entre as propostas recebidas.

OrçamentoestimadoeplanilhasdequantitativosepreçosunitáriosconformeANEXOIV.

20. VIGÊNCIA DO CONTRATO

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. CONSIDERAÇÕESGERAIS

AexecuçãodosserviçosobjetodesteTermodeReferência,incluindosuasimplementações,deverá, obrigatoriamente, ser efetuada de forma a não afetar o funcionamento dos serviços já em operação;

Nocasodenecessidadedeinterrupçãodeoutrosserviçosouequipamentos,emdecorrênciadainstalaçãoaser efetuada, esta deverá ser devidamente planejada e acordada com a PRODEB;

Osserviços,objetodestalicitação,deverãoserexecutadossobainteiraresponsabilidadefuncionaleoperacional da CONTRATADA, sobre cujos empregados deverá manter estrita e exclusiva fiscalização;

AprestaçãodosserviçosnãogeravínculoempregatícioentreosempregadosdaCONTRATADAeos CONTRATANTES, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta;

TodaaequipedeprofissionaisdaCONTRATADAdeveráportaridentificaçãoquandodaexecuçãodosserviços;

TodaaequipedeprofissionaisdaCONTRATADAdeveráusarequipamentodesegurançaconformecadaatividade a ser efetuada;

Asdiscrepâncias,dúvidas,omissõesouerrosobservadosdevemserlevadosaoconhecimentodoCONTRATANTE, 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. OBRIGAÇÕESCONTRATUAIS

OBRIGAÇÕESDACONTRATADA

ZelarpelocumprimentodoobjetoedasdemaiscláusulasdesteTermodeReferênciaeContrato;

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;

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;

Prestar os serviços de garantia e suporte no sistema 24x7 (vinte e quatro horas por dia, sete dias na semana);

Utilizar cópias legais de software, sistemas operacionais e outros necessários para a realização de suas instalações;

Atender às solicitações de serviços de acordo com as especificações técnicas, cronogramas e condições especificadas;

Prestar os serviços com pessoal adequadamente capacitado em locais e instalações de acordo com as orientações constantes neste Termo de Referência;

Dispor de pessoal necessário para garantir a execução dos serviços, nos regimes contratados, sem interrupçãosejapormotivodeférias,descansosemanal,licença,falta aoserviço,greve,demissãoeoutros análogos, obedecidas às disposições da legislação trabalhista vigente;

Não veicular publicidade ou qualquer outra informação acerca das atividades objeto deste contrato, sem prévia autorização da CONTRATANTE;

Manter, durante a vigência do contrato, todas as condições de habilitação e qualificação exigidas neste Termo de Referência;

Assumir todas as providências e obrigações estabelecidasnasnormasde segurança e legislação específicadeacidentes 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;

Assumir todas as despesas e ônus relativos ao seu pessoal, ficando ainda, para todos os efeitos legais, expressospelaCONTRATADA,ainexistênciadequalquervínculoempregatícioentreseusempregadose/ou prepostos do CONTRATANTE;

Promover a transferência do conhecimento vide (hands-on) de cada produto entregue, para os profissionais da CONTRATANTE, sem ônus adicional;

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;

Dar ciência a CONTRATANTE, imediatamente e por escrito, de qualquer anormalidade identificada na execução dos serviços;

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 vazamentodeinformação,decorrentesdeaçãodanosaoculposa,nasformasdenegligência,imprudência ou imperícia, venha a ocasionar a PRODEB ou a terceiros;

Responsabilizar-se pelo perfeito funcionamento do objeto do contrato, arcar com os eventuais prejuízos causadosàCONTRATANTEe/ouaterceiros,provocadosporineficiênciaouirregularidadecometidaporseus 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;

Reparar, exclusivamente às suas custas, todos os defeitos, erros, falhas, omissões e quaisquer irregularidades verificadasnoshardwares, softwaresfornecidose nos serviços, bem comoresponsabilizar- se por qualquer dano ou prejuízo daí decorrente;

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.

OBRIGAÇÕESDACONTRATANTE

PRODEB

Operareadministrarassoluçõesadquiridas;

Fiscalizar o cumprimento do objeto e das demais cláusulas deste Termo de Referência e seus anexos;

ProporcionarascondiçõesnecessáriasparaqueaCONTRATADApossacumpriroqueestabelece este Termo de Referência e seus anexos;

ReceberoobjetonoprazoecondiçõesestabelecidasnopresenteTermodeReferência;

Verificarminuciosamente,noprazofixado,aconformidadedosbensrecebidosprovisoriamente com as especificações constantes do Termo de Referência e da proposta, para fins de aceitação e recebimento definitivo;

ComunicaràCONTRATADA,porescrito,sobreimperfeições,falhasouirregularidadesverificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de comissão/servidor especialmente designado;

ProporcionarascondiçõesnecessáriasparaqueaCONTRATADApossacumpriroqueestabelece este Termo de Referência e seus anexos;

Designarpessoasparaospapéisdescritosquantoàfiscalização;

Convocar,realizareregistrarreuniõesjuntoàCONTRATADA;

Atestarehomologaraentregadoshardwaresesoftwaresentregues;

Validaraexecuçãodosserviçosaseremprestados;

Notificar formalmente a CONTRATADA quanto a defeitos ou irregularidades observadas nos hardwares,softwaresenaexecuçãodosserviçose sobreaaplicaçãodepenalidades,asseguradasua prévia defesa;

Permitir a entrada dos funcionários da CONTRATADA, desde que devidamente identificados, garantindoquetenhamacessoaosequipamentos, bemcomofornecertodososmeiosnecessáriosà execução dos serviços;

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;

Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos profissionais da CONTRATADA ou o seu Preposto;

Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da CONTRATADA, conforme determina a Lei, antes de efetuar o pagamento devido.

ÓRGÃOSEENTIDADESDAADMINISTRAÇÃOPÚBLICADOESTADODABAHIA:

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. OBRIGAÇÕESDOGESTORTÉCNICODASOLUÇÃO–PRODEB

Exerceragestãotécnicadosserviçosdeprofissionaisedemonitoramento,conformeobjetodesteEdital;

Exerceroplanejamentoeanálisedaarquiteturadassoluçõesdesegurançanecessárias;

24. PROTEÇÃODEDADOSPESSOAIS

ACONTRATADA 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;

ACONTRATADA 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;

ACONTRATADAdeveassegurar-sedequetodososseuscolaboradores,consultorese/ouprestadoresdeserviços que,noexercíciodassuasatividades,tenhamacessoe/ouconhecimentodainformaçãoe/oudosdadospessoais, respeitem o dever de proteção, confidencialidade e sigilo;

ACONTRATADA 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;

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 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;

ACONTRATADA 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;

ÀCONTRATADA não será permitido deter cópiasou backups, informação, dados pessoaise/ou basededadosa que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual;

ACONTRATADAdeveráeliminarosdadospessoaisaquetiverconhecimentooupossseemrazãodocumprimento do objeto deste instrumento contratual tão logo não haja mais necessidade de realizar seu tratamento;

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 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;

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;

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;

O dever de sigilo e confidencialidade, e as demais obrigações descritas na presente cláusula, permanecerão em vigorapósaextinçãodasrelaçõesentreACONTRATADAeaCONTRATANTE,bemcomo,entreACONTRATADAe osseuscolaboradores,subcontratados,consultorese/ouprestadoresdeserviçossobpenadasançõesprevistas na Lei nº 13.709/2018, suas alterações e regulamentações posteriores, salvo decisão judicial contrária;

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 outraspenalidades.

25. ELEMENTOSNECESSÁRIOSÀGESTÃODOCONTRATO

ParaagestãoefiscalizaçãodocontratoseráadotadooritoprevistonoCapítuloV,SeçãoIII,doRegulamentode Licitações e Contratos da PRODEB. O Gestor e Fiscal do contrato decorrente deste processo serão indicados no momento da contratação.

26. FORMADECOMUNICAÇÃO

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. SANÇÕESADMINISTRATIVAS

Serãoaplicadas sançõesadministrativasao Licitante quecometer 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. TERMODECOMPROMISSOEDECONFIDENCIALIDADE

ACONTRATADA compromete-se a cumprir e obedecer à Política de Segurança da Informação do Governo do Estadoda Bahia;

A CONTRATADA deverá assinar Termo de Compromisso, Sigilo e Confidencialidade, Anexo I deste Termo no momento da assinatura do contrato.

29. GARANTIACONTRATUAL

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 ContratosdaPRODEB,ficandoesclarecidoqueagarantiacontratualdeveráterseuvaloratualizadonasmesmas condições do contrato e renovada, quando for o caso, conforme previsto neste Termo de Referência.

30. MATRIZDERISCO

Este Termo de Referência foi elaborado com base nos dados levantados e explicitados no documento denominado MAPA DE RISCOS.

Salvador,03deabrilde2024.

ANEXO I

TERMODECOMPROMISSO,SIGILOECONFIDENCIALIDADE

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 denominadaCONTRATANTE,e de outrolado_, CNPJ nº

/,situadanacidadede_,àRua:_, bairro_,doravantedenominadaCONTRATADA,têmentresijusta eacertada,acelebraçãodo presente TERMO DE SIGILO E CONFIDENCIALIDADE, através do qual a CONTRATADA aceita não divulgar sem autorizaçãopréviae formalsegredos einformações sensíveisdepropriedade daPRODEB ede seusclientese se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

PRIMEIRA–ACONTRATADAreconhecequeemrazãodassuasatividadesprofissionais, estabelececontato com informações sigilosas, que devem ser entendidas como segredo. Estas informações devem ser tratadas confidencialmentesobqualquercondiçãoenãopodemserdivulgadasaterceirosnãoautorizados,aíseincluindo os próprios Colaboradores da CONTRATADA, sem a expressa e escrita autorização daCONTRATANTE;

SEGUNDA - As informações a serem tratadas confidencialmente são aquelas assim consideradas no âmbito da PRODEB,transmitidaspormeiosescritos,eletrônicos, verbaisouquaisqueroutros, eque, porsuanatureza,não são ou não deveriam ser de conhecimento de terceiros, tais como:

1. Todainformaçãorelacionadaacomputadorecomponentesdesoftwareemgeral,programasexistentes (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 erotinas;

2. Documentos,informaçõesedadosarmazenadosdeatuaçãoconsultivaecontenciosa,deestratégiasou 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. Númerosevaloresfinanceirosdaempresataiscomo:inadimplência,relaçãodesalários, fluxodecaixa, informações de custos, dentre outros;

6. Informaçõesreferentesadadospessoaise/oudadospessoaissensíveis;

TERCEIRA –A CONTRATADAreconhecequea lista acima é meramente exemplificativa e ilustrativa equeoutras hipótesesdeconfidencialidadequejáexistamouquevenhamasurgirnofuturodevemsermantidassobsegredo.Em casodedúvidaacercadaconfidencialidadededeterminadainformaçãoaCONTRATADAdevetrataramesmasob 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-ACONTRATADAestácientedequeoserviçodecorreioeletrônicocorporativo,casosejafornecidopela 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–ACONTRATADAreconheceque,aotérminodopresentecontrato_, 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–ACONTRATADAdeve assegurarquetodososseuscolaboradoresguardarão sigilo sobreasinformações que porventura tiverem acesso, e que os mesmos se comprometem a informar imediatamente ao seu superior hierárquico,qualquerviolaçãodasregrasde sigilo,porpartedeleoudequalquerpessoa,inclusivenoscasosde violação não intencional;

ParágrafoPrimeiro:AapresentaçãodosTermosdeSigiloeConfidencialidadedeseuscolaboradoresnãoexime a CONTRATADA das penalidades por violação das regras por parte destes;

Parágrafosegundo:ACONTRATADAdeveráfornecercópiadetodososTermosfirmadoscomseuscolaboradores à CONTRATANTE no prazo de 10 (dez) dias após assinatura dos respectivos termos;

ParágrafoTerceiro:SemprequeumcolaboradorforadmitIdo,ACONTRATADAdeverá fornecercópiados novos termos firmados no prazo de 2 (dois) dias após assinatura dos respectivostermos;

SÉTIMA-OatendimentodesteTermodeSigiloeConfidencialidadebemcomodadasDiretrizesBásicasdaPolítica deSegurança da Informação devem ser incorporadosformalmente ao contrato detrabalho dosfuncionáriosda 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 docontratoAA/NNNN-00,eabrangem,alémdasinformaçõesdequevenhaatomar 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;

ANEXO II MODELODEPROPOSTA

ITENSDESOFTWAREEHARDWARE					
ITEM	**DESCRITIVO**	**UNID**	**QTD**	**VALORUNITARIO**	**VALOR TOTAL**
01	SoluçãodeSegurançadeEndpoint-EPP	UN	2500		
02	SoluçãoparaduploFatordeAutenticação-TokenMobile	UN	750		
03	SoluçãodeSegurançadeRedeNGFWTIPOI	UN	450		
04	SoluçãodeSegurançadeRedeNGFWTIPOII	UN	60		
05	SoluçãodeSegurançadeAplicaçõesWAFTIPOI	UN	08		
06	SoluçãodeSegurançadeAplicaçõesWAFTIPOII	UN	02		
07	SoluçãodeSegurançaDecoy/Honeypot	UN	04		
08	SoluçãodeSegurançadeEmail.	UN	02		
VALORTOTALAQUISIÇÃO(A)				R$	

ITENSDESERVIÇO					
ITEM	**DESCRITIVO**	**UNID**	**QTD**	**VALORUNITARIOMENSAL**	**VALORTOTALMENSAL**
09	ServiçosProfissionaisdeMonitoramentoeSegurançadoDatacenter da PRODEB pelo período de 24 Meses.	UN	1		
10	Serviços Profissionais de Monitoramento e Segurança para o item “SoluçãodeSegurançadeEndpoint-EPP”paracadaitem monitoradopeloperíodode24Meses.	UN	62.500		
11	Serviços Profissionais de Monitoramento e Segurança para o item “Solução para duplo Fator de Autenticação - Token Mobile”	UN	3.750		

	para cada item monitorado pelo período de 24 Meses.				
12	ServiçosProfissionaisdeMonitoramentoeSegurançaparaositens “SoluçãodeSegurançadeRedeNGFWTIPOI,II”paracadaitem monitoradopeloperíodode24Meses.	UN	510		
13	Serviços Profissionais de Monitoramento e Segurança para o item “SoluçãodeSegurançadeAplicaçõesWAFTIPOI”paracadaitem monitoradopeloperíodode24Meses.	UN	08		
VALORTOTALMENSALSERVIÇOS(B) PAGAMENTOMENSAL				R$	
VALORTOTALPARA24MESES(C) VALORTOTALMENSALSERVIÇOS(B)X24(vinteequatro)MESES				R$	

VALORGLOBALDO LOTE VALORTOTALAQUISIÇÃO(A)+VALORTOTALPARA24MESES(C)	R$

Declaramosquetemosconhecimento econcordamoscomtodosositens mencionadosno TermodeReferência, 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 qualquernatureza,materiaisempregados,inclusiveferramentas,utensílioseequipamentosutilizados,

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

CARIMBODOFORNECEDOR (COMCNPJ)	RAZÃOSOCIAL	
	TELEFONE	PRAZODEENTREGA
	DATA	VALIDADEDAPROPOSTA
	CONTATO	E-MAIL

ANEXOIII

SOLUÇÕESDESEGURANÇAINSTALADASNAPRODEB

Produto	Descrição	PartNumber	Qtd.
FortiAnalyzer3700F	SoluçãodeLogseRelatoria	FAZ-3700F	2
FortiAnalyzer2000E	SoluçãodeLogseRelatoria	FAZ-2000E	2
FortiAuthenticator3000E	SoluçãodeAutenticaçãoCentralizada	FAC-3000E	2
FortiManager3000G	SoluçãodeGerênciaCentralizada	FMG-3000G	1
FortiManager3900E	SoluçãodeGerênciaCentralizada	FMG-3000G	1
FortiSIEM	SoluçãodeCorrelaçãodeeventos,Resposta AutomáticaeRemediaçãodeIncidentes	FSM-AIO-BASE	1
FortiWeb-2000F	SoluçãodeFirewalldeaplicaçõesWEB	FWB-2000F	1
FortiADC400F	SoluçãodeBalanceamentodeCargadeAplicações	FAD-400F	2
FortiGate-3301E	SoluçãodeNextGenerationFirewall-NGFW	FG-3301E	2
SoluçãoTrendMicro™ DeepDiscovery™Inspector	SoluçãodeNetworkDetectionandResponse	DDI9000	2
NS9500Sensor	SoluçãodeIntrusionPreventionSystem	NS9500	2
TrendWorkloadSecurity	AgenteXDRdesegurançadeservidores		2250
TrendEndpointSensor	AgenteXDRdesegurançaparadesktops		500
Fortigate600D	SoluçãodeNextGenerationFirewall–NGFW	FG-600D	2
Fortigate600F	SoluçãodeNextGenerationFirewall–NGFW	FG-600F	2
Fortigate3000D	SoluçãodeNextGenerationFirewall–NGFW	FG-3000D	2

Fortigate3700F	SoluçãodeNextGenerationFirewall–NGFW	FG-3700F	2
Tenable.SC	SoluçãodeAnáliseeVulnerabilidadede Infraestrutura		1
Tenable.io	SoluçãodeAnáliseeVulnerabilidadedeAplicações		1
Webgateway	SoluçãodeProxyemódulos	WG-5500D	6
ePOTrellix	SoluçãodeGerenciamentodeEDRemódulos		
EDRTrellix	SoluçãodeEDRemódulos		
Forescout	SoluçãodeVisibilidade,AutomaçãoeControlede Acesso		1

ANEXOIV

TABELADEVALORESREFERENCIAIS

ITEM	DESCRITIVO	UNID	QUANTIDADE
1	SoluçãodeSegurançadeEndpoint–EPP.Cod.SIMPAS(70510900007796-8)	UN	2500
2	SoluçãoparaduploFatordeAutenticação-TokenMobile.CodSIMPAS(70510900007800-0)	UN	750
3	SoluçãodeSegurançadeRedeNGFWTIPOICod.SIMPAS(70510900007797-6)	UN	450
4	SoluçãodeSegurançadeRedeNGFWTIPOII.Cod.SIMPAS(70510900007798-4)	UN	60
5	SoluçãodeSegurançadeAplicaçõesWAFTIPOI.Cod.SIMPAS(70510900007793-3)	UN	8
6	SoluçãodeSegurançadeAplicaçõesWAFTIPOII.Cod.SIMPAS(70510900007794-1)	UN	2
7	SoluçãodeSegurançaDecoy/Honeypot.CodSIMPAS(70510900007799-2)	UN	4
8	SoluçãodeSegurançadeEmail.–Cod.SIMPAS(70510900007795-0)	UN	2
9	ServiçosProfissionaisdeMonitoramentoeSegurançadoDatacenterdaPRODEBpeloperíodode24Meses.–Cod.SIMPAS(02240900007805-0)	UN	1
10	ServiçosProfissionaisdeMonitoramentoeSegurançaparaoitem“SoluçãodeSegurançadeEndpoint-EPP”paracadaitemmonitorado pelo período de 24 Meses. Cod SIMPAS (02240900007804-2)	UN	62.500
11	ServiçosProfissionaisdeMonitoramentoeSegurançaparaoitem“SoluçãoparaduploFatordeAutenticação-TokenMobile”para cada item monitorado pelo período de 24 Meses. Cod SIMPAS (02240900007803-4)	UN	3.750
12	ServiçosProfissionaisdeMonitoramentoeSegurançaparaositens“SoluçãodeSegurançadeRedeNGFWTIPOI,II”paracadaitem monitorado pelo período de 24 Meses. Cod SIMPAS (02240900007802-6)	UN	510
13	ServiçosProfissionaisdeMonitoramentoeSegurançaparaoitem“SoluçãodeSegurançadeAplicaçõesWAFTIPOI”paracadaitem monitorado pelo período de 24 Meses. Cod. SIMPAS (02240900007801-8)	UN	8
VALOR TOTAL			

ANEXOV

PLANILHADEQUANTITATIVOSDOSÓRGÃOSEENTIDADESPARTICIPANTES

SIGLA	ÓRGÃO/ENTIDADE	ITEM01	ITEM02	ITEM03	ITEM04	ITEM05	ITEM10	ITEM11	ITEM12	I
ADAB	AgênciadeDefesaAgropecuáriadaBahia	79	2	0	0	0	1975	10	0	
AGERBA	AgênciaEstadualdeRegulaçãoServiçosPúblicosde Energia Transporte	16	4	2	0	0	400	20	2	
AGERSA	AgênciaReguladoradeSaneamentoBásicodo EstadodaBahia	6	8	0	2	0	150	40	2	

CASACIVIL	CasaCivildoGovernodoEstadodaBahia	19	10	2	2	2	475	50	4	
CASAMILITAR	CasaMilitardoGovernadordaBahia	8	2	0	0	0	200	10	0	
CBM	CorpodeBombeirosMilitardaBahia	2	0	0	0	0	50	0	0	
DPT	DepartamentodePolíciaTécnicadaBahia	53	0	2	2	0	1325	0	4	
FAPESB	FundaçãodeAmparoàPesquisadoEstadodaBahia	6	25	0	1	0	150	125	1	
FPC	FundaçãoPedroCalmon/SECULT	16	0	0	2	0	400	0	2	
GABGOV	GabinetedoGovernadordoEstadodaBahia	16	7	2	2	0	400	35	4	
IPAC	InstitutodoPatrimônioArtísticoeCulturaldo EstadodaBahia/SECULT	9	0	0	0	0	225	0	0	
IRDEB	InstitutodeRadiodifusãoEducativadaBahia/ SECULT	1	0	2	0	0	25	0	2	
PGE	ProcuradoriaGeraldoEstadodaBahia	1	1	2	2	2	25	5	4	
PLANSERV	SistemadeAssistênciaàSaúdedosServidores Públicos Estaduais	14	0	2	0	0	350	0	2	
PMBA	PolíciaMilitardaBahia	158	40	85	2	0	3950	200	87	
SAEB	SecretariadaAdministraçãodoEstadodaBahia	106	60	2	4	0	2650	300	6	
SDE	SecretariadeDesenvolvimentoEconômicodo EstadodaBahia	1	0	0	1	0	25	0	1	
SDR	SecretariadeDesenvolvimentoRuraldoEstadoda Bahia	1	0	0	1	0	25	0	1	
SEAGRI	SecretariadaAgricultura,IrrigaçãoeReforma Agrária	11	40	1	2	0	275	200	3	
SEAP	SecretariadeAdministraçãoPenitenciáriae RessocializaçãodoEstadodaBahia	1	0	20	4	0	25	0	24	
SEC	SecretariadaEducaçãodoEstadodaBahia	1470	440	271	18	2	36750	2200	289	
SECTI	SecretariadeCiência,TecnologiaeInovaçãodo Estado da Bahia	1	0	0	2	0	25	0	2	
SEDUR	SecretariadeDesenvolvimentoUrbanodaBahia	16	0	0	1	0	400	0	1	
SEI	SuperintendênciadeEstudosEconômicoseSocias da Bahia	25	3	2	2	0	625	15	4	0
SERIN	SecretáriadeRelaçõesInstitucionaisdoEstadoda Bahia	13	0	0	1	0	325	0	1	0
SESAB	SecretariadeSaúdedoEstadodaBahia	344	100	33	4	0	8600	500	37	0
SETRE	SecretariadoTrabalho,Emprego,RendaeEsporte doEstadodaBahia	59	0	20	0	0	1475	0	20	0
SETUR	SecretariaEstadualdeTurismodaBahia	11	0	0	0	0	275	0	0	0
SJDH	SecretariadeJustiçaeDireitosHumanos	24	0	1	0	0	600	0	1	0
SSP	SecretariadeSegurançaPública	4	4	0	1	2	100	20	1	2
SUFOTUR	SuperintendênciadeFomentoaoTurismodaBahia	6	2	0	2	0	150	10	2	0
VICEGOV	GabinetedoVice-Governador	3	2	1	2	0	75	10	3	0
TOTAL		**2500**	**750**	**450**	**60**	**8**	**62500**	**3750**	**510**	**8**

AUGUSTO SÉRGIO VASCONCELOS DE OLIVEIRA
SECRETARIA DO TRABALHO, EMPREGO, RENDA E ESPORTE – SETRE

RICARDO LUIZ DE OLIVEIRA
CONSÓRCIO CYBERSEC BAHIA

ALEXANDRE RODRIGO CRUZ RIOS CORUJEIRA DE BRITTO
CONSÓRCIO CYBERSEC BAHIA

Testemunhas:

CPF: CPF:

Documento assinado eletronicamente por **Alexandre Rodrigo Cruz Rios Corujeira de Britto**, **Usuário Externo**, em 19/05/2025, às 15:24, 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 19/05/2025, às 16:44, 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 **Augusto Sérgio Vasconcelos de Oliveira**, **Secretário**, em 22/05/2025, às 16:33, 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.

Documento assinado eletronicamente por **Tiago Cerqueira Santos**, **Testemunha**, em 22/05/2025, às 17:22, 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 **00110803227** e o código CRC **B0B56354**.

Referência: Processo nº 021.2142.2024.0005465-03 SEI nº 00110803227

DIÁRIO OFICIAL
República Federativa do Brasil - Estado da Bahia
SALVADOR, **SEXTA-FEIRA**, 23 DE MAIO DE 2025 - ANO CIX - Nº 24.161

RESUMO CONTRATO Nº. 002/2025 PROCESSO SEI Nº: 019.8721.2025.0023160-14. DISPENSA DE LICITAÇÃO Nº. 0008/2025. CONTRATANTE: ESTADO DA BAHIA, ATRAVÉS DA SECRETARIA DA SAÚDE - SESAB. OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS DE LOCAÇÃO DE CATRACAS PARA CONTROLE DE ACESSO NAS RECEPÇÕES DA MATERNIDADE ALBERT SABIN. CONTRATADA: TIC MOBILE SOLUCOES EM TECNOLOGIA DA INFORMACAO COMUNICACAO E REPRESENTACAO LTDA. VALOR GLOBAL: R$ 44.160,00 (QUARENTA E QUATRO MIL CENTO E SESSENTA REAIS). VIGÊNCIA: 12 (DOZE) MESES, A PARTIR DE 21/05/2025 A 21/05/2026. DOTAÇÃO ORÇAMENTÁRIA: UNIDADE GESTORA: 19.601/76. FONTE DE RECURSO: 130/281. ATIVIDADE: 2641. ELEMENTO DE DESPESA: 33903900. REGIME DE EXECUÇÃO: SERVIÇO COM EMPREITADA POR PREÇO GLOBAL DATA DE ASSINATURA: 21/05/2025.

MATERNIDADE ALBERT SABIN-MAS

RESUMO - AUTORIZAÇÃO DE FORNECIMENTO DE MATERIAL (AFM)/AUTORIZAÇÃO DE PRESTAÇÃO DE SERVIÇO (APS) - MODALIDADE REGISTRO DE PREÇO, PREGÕES ELETRÔNICOS E DISPENSA DE LICITAÇÃO

AFM/APS 19.134	FORNECEDOR	CNPJ	OBJETO	VALOR	DATA ASSINATURA
00198/2025	SE LIGUE ACESSORIOS E ELETRONICOS LTDA	51.515.743/0001-35	MATERIAL DE ESCRTÓRIO	R$ 480,00	20/05/2025
00174/2025	MMX EMPREENDIMENTOS E SERVICOS LTDA	10.710.394/0001-25	MATERIAL HOSPITALAR	R$ 646,00	20/05/2025
00178/2025	RITA MARIA CONCEICAO SILVA	13.372.912/0001-36	MATERIAL DE ESCRTÓRIO	R$ 998,00	20/05/2025
00192/2025	MEDISIL MEDICAMENTOS LTDA	96.827.563/0001-27	MATERIAL HOSPITALAR	R$ 379,00	20/05/2025
00201/2025	RIOBAHIAFARMA COMERCIO E DISTR DE PRODUTOS MEDICOS E COSMETICOS LTDA	15.145.035/0001-96	MEDICAMENTOS	R$ 1.982,00	21/05/2025
00191/2025	UNI HOSPITALAR LTDA	07.484.373/0001-24	MEDICAMENTOS	R$ 82.545,50	21/05/2025
00204/2025	M MED COMERCIAL DE MEDICAMENTOS E PRODUTOS HOSPITALARES LTDA	28.387.424/0001-70	MATERIAL HOSPITALAR	R$ 260,00	21/05/2025
00207/2025	OTTO PEREIRA COMERCIO ATACADISTA DE EMBALAGENS LTDA	50.164.737/0001-18	EMBALAGEM	R$ 6.418,80	21/05/2025
00209/2025	OTTO PEREIRA COMERCIO ATACADISTA DE EMBALAGENS LTDA	50.164.737/0001-18	EMBALAGEM	R$ 1.897,35	21/05/2025
00210/2025	OTTO PEREIRA COMERCIO ATACADISTA DE EMBALAGENS LTDA	50.164.737/0001-18	EMBALAGEM	R$ 1.935,00	21/05/2025
00197/2025	CONTUDO LICITAÇÕES LTDA	44.145.169/0001-05	MATERIAL DE ESCRTÓRIO	R$ 1.051,63	21/05/2025
00164/2025	JF ANDAIMES COMERCIO E SERVICOS LTDA	24.576.901/0001-94	MATERIAL MANUTENÇÃO	R$ 170,00	21/05/2025
00211/2025	CEI COMERCIO EXPORTACAO E IMPORTACAO DE MATERIAIS MEDICOS LTDA	40.175.705/0001-64	MATERIAL HOSPITALAR	R$ 2.100,00	22/05/2025

Salvador, 22 de Maio de 2025. Louricea de Cerqueira Daltro/Diretora Geral /MAS

SECRETARIA DA SEGURANÇA PÚBLICA

Polícia Militar da Bahia – PM/BA

TERMO DE RECONHECIMENTO DE DÉBITO, INDENIZAÇÃO E QUITAÇÃO DE CRÉDITOS Nº 001/2025 - SSP/PMBA/CPRC-C.

Processo Administrativo SEI nº 030.12260.2025.0065657-68. Termo de Reconhecimento de Débito CPRC-C n.º 00111792192/2025. O Estado da Bahia, através da Polícia Militar, reconhece que é devido à Empresa Baiana de Águas e Saneamento (EMBASA), em razão da prestação do serviço de fornecimento de água potável na sede da 47ª CIPM, situado na Rua Luciana Barbosa, s/n, Jardim Cajazeiras, Salvador - Ba, no valor total de R$ 176,90 (cento e setenta e seis reais e noventa centavos). Dotação Orçamentária - Projeto/Atividade: 4514; Elemento de Despesa: 3.3.90.39.000. Salvador, 22 de maio de 2025. Antonio Carlos Silva Magalhães - Cel PM - Comandante Geral.

Corpo de Bombeiros Militar da Bahia - CBM/BA

RESUMO DE TERMO ADITIVO Nº 003/2025 AO CONTRATO Nº 011/2024 - SUBCOMANDO-GERAL.
Processo Administrativo nº089.8516.2025.0019279-21. Contratante: CORPO DE BOMBEIROS MILITAR DO ESTADO DA BAHIA, CNPJ nº 22.306.987/0001-00. Contratada BRASPE RECURSOS HUMANOS EIRELI, CNPJ nº 03.595.040/0001-11. Objeto: Constitui objeto do presente aditivo a Alteração da Cláusula Nona - Fiscalização do Contrato indicado no preâmbulo, com fundamento no art. 154 da Lei no 9.433/05. Permanece como Gestor deste Contrato, a servidora FABIANA SILVEIRA ARAGÃO - TEN BM (SCG), matrícula: 89.640.142-0. Permanecem indicados como fiscais os seguintes servidores: 1º Batalhão de Bombeiro Militar: MICHEL DE FREITAS SANTOS - CB BM, Mat.: 30.506.709. 13º Batalhão de Bombeiro Militar: - ANTONIO MARCOS ARAÚJO ANDRADE - SUB TEN BM, Mat.: 30.299.480-0. Coordenação de Saúde: - NÚBIA PEREIRA DA SILVA - SGT BM, Mat.: 30.340.578-1. 12º Batalhão de Bombeiro Militar: - ANA LÚCIA AMORIM FERREIRA - SUB TEN BM, Mat.: 30.294.201-5. Ficam indicadas como novas fiscais(inclusão) as servidoras: CLAUDIANE DANTAS CONCEIÇÃO - SD BM, Mat.: 89.644.343-0 vinculada a Coordenação de Saúde e a servidora MARISA CONCEIÇÃO DOS SANTOS - SD BM, Mat.: 89.653.968 vinculada ao 1ºBBM. Data da assinatura: 22/05/2025. ALOISIO MASCARENHAS FERNANDES - CEL BM COMANDANTE GERAL DO CBMBA.

SECRETARIA DO TRABALHO, EMPREGO, RENDA E ESPORTE

RESUMO DO CONTRATO N. 016/2025

Processo SEI n. 021.2142.2024.0005465-03. Pregão Eletrônico - Registro de Preço 006/2024. Contratante: Estado da Bahia/SETRE. Contratada: CONSÓRCIO CYBERSEC BAHIA. 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 data center PRODEB. PRAZO: será de 28 (vinte e oito) meses, a contar da data da sua assinatura. REGIME DE EXECUÇÃO: Serviço com empreitada por preço global. DO PREÇO: **R$337.920,00** (trezentos e trinta e sete mil e novecentos e vinte reais). Dotação Orçamentária:

UNIDADE ORÇAMENTÁRIA	FONTE/BA	PAOE	NATUREZA DA DESPESA	UNIDADE GESTORA
3.21.101 - APG	0.100	2002	33.90.30.000 33.90.40.000	0003 - DA
3.21.602 - FET/BA	0.100	2002	33.90.30.000 33.90.40.000	0001 - FET/BA

Assinam: Augusto Sergio Vasconcelos de Oliveira - Secretário da SETRE e representantes da Contratada: Ricardo Luiz De Oliveira e Alexandre Rodrigo Cruz Rios Corujeira de Britto.

APOSTILA Nº 007/2025

O SECRETÁRIO DO TRABALHO, EMPREGO, RENDA ESPORTE, no uso de suas atribuições e considerando o que dispõe o inciso I do Art. 135 da Lei Estadual nº 9.433/2005, RESOLVE expedir a presente Apostila para **alterar a dotação orçamentária do Contrato nº 24/2019**, celebrado com a **Associação Fábrica Cultural**, que tem como objeto a **gestão dos serviços de Qualificação dos Artesãos baianos**, **incluindo a promoção e comercialização da produção artesanal**, que para fins de execução das despesas passa a vigorar de acordo com a dotação orçamentária abaixo:

UNIDADE ORÇAMENTÁRIA	FONTE	PAOE	NATUREZA DA DESPESA	UNIDADE GESTORA
3.21.101 - APG	0.100	2234	33.50.85.000	0009 - CFA

GABINETE DO SECRETÁRIO, em 22 de maio de 2025.
AUGUSTO SÉRGIO VASCONCELOS DE OLIVEIRA
Secretário

EGBA CERTIFICAÇÃO DIGITAL
EGBA: 71 3343-2886 • www.egba.ba.gov.br