PRODEPA

CONTRATO Nº 022/2025

CONTRATO DE AQUISIÇÃO DE SOLUÇÃO FIREWALL, COM TREINAMENTO E SERVIÇOS TÉCNICOS ESPECIALIZADOS COM INSTALAÇÃO, CONFIGURAÇÃO, OPERAÇÃO ASSISTIDA E CONTINUADA, QUE FAZEM ENTRE SI, EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO PARÁ PRODEPA E ALLTECH SOLUÇÕES EM TECNOLOGIA LTDA, COMO MELHOR ABAIXO SE DECLARA.

1. CLÁSULA PRIMEIRA - PARTES

A EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO PARÁ - PRODEPA, Empresa Pública, com personalidade jurídica própria de direito privado, constituída na forma da Lei Estadual n.º 5.460/88, inscrita no CNPJ sob o n.º 05.059.613/0001-18, Inscrição Estadual n.º 15.271.0884, com sede na Rodovia Augusto Montenegro, km 10, Centro Administrativo do Estado, Icoaraci – Belém - Pará, CEP 66820-000, neste ato representada por seu Presidente o Prof. Dr. CARLOS EDILSON DE ALMEIDA MANESCHY, brasileiro, casado, RG nº 4.059.742 SSP/PA, CPF nº 066.166.902-53, residente na Rua Conselheiro Furtado, nº 2905, Apt. 901 - Cremação, Cep: 66.040-100, Belém - Pará, nomeado através de Decreto Governamental, publicado no DOE nº 35.276, de 02.02.2023, doravante designada CONTRATANTE, e ALLTECH SOLUÇÕES EM TECNOLOGIA LTDA, com sede Brasilia, Distrito Federal, sito SCN Quadra 01 Bloco F – Salas 802 a 810 – Ed. America Office Tower, bairro Asa Norte, Cep 70711060, inscrita no CNPJ nº 21.547.011/0001-66, Inscrição Estadual n º 07.704.559/001-89, representada neste ato por seu Proprietário Sr. MURILO ROSSETTO, Brasileiro, casado, portador da Cédula de Identidade nº 2485039 - SSP/DF, inscrito no CPF 03603182154, Diretor Comercial, residente e domiciliado na Rua das Paineiras, LT.04 Apt. º 1807 Bairro Taguatinga-DF, CEP 71.929-918., doravante designada CONTRATADA, resolvem celebrar o presente contrato, mediante as cláusulas e condições a seguir enunciadas.

2. CLÁSULA SEGUNDA - FUNDAMENTO LEGAL

2.1. O presente contrato é oriundo do Pregão Eletrônico SRP nº 9003/2024, constante no Processo PAE nº 2023/1410882 e o Processo PAE 4.0 2025/2623042, da Lei Federal nº. 13.303/2016 (Estatuto jurídico das empresas públicas, das sociedades de economia mista e de suas subsidiárias, no âmbito da União, Estados, DF e Municípios); Decreto nº. 2.121/2018 (Institui normas gerais de licitações e contratos da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito do Estado do Pará); Regulamento Interno de Licitações e Contratos — RILC — da PRODEPA; Lei Estadual nº. 6.474/2002 (Institui, no Estado do Pará, a modalidade de licitação denominada pregão); Decreto Estadual nº. 2.940/2023 (Regulamento o uso do pregão eletrônico no Estado), atualizado pelos Decretos Estaduais nº. 3.897/2024 e nº 3.804/2024; Lei Estadual nº. 8.417/2016 (Estatuto da Microempresa e EPP); Instrução Normativa SLTI/MPOG nº. 3/2018 (Estabelece regras de funcionamento do Sistema de Cadastramento Unificado de Fornecedores – SICAF, no âmbito do Poder Executivo Federal); Lei Complementar Federal nº. 123/2006 (Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte); demais normas aplicáveis e as condições estabelecidas neste Edital.

3. CLÁUSULA TERCEIRA - OBJETO

3.1. O objeto do presente instrumento é a **AQUISIÇÃO DE SOLUÇÃO FIREWALL** com treinamento e serviços técnicos especializados com instalação, configuração, operação assistida e continuada pelo período de 36 (trinta e seis) meses, conforme descrito no Termo de Referência, o qual adere a este documento para todos os fins.

3.2. Este instrumento se vincula ao edital licitatório citado na Cláusula 2, à proposta do licitante vencedor, e aos anexos desses documentos.

3.3. Os equipamentos e serviços cobertos por esta contratação são os seguintes itens descritos no Termo de Referência:

ITEM	DESCRIÇÃO	MARCA/MODELO	QTD	VALOR UNITÁRIO	VALOR TOTAL
3	Equipamentos do tipo "firewall" de nova geração (NGFW) – TIPO 3	FORTINET/ FG-80F	8	R$ 42.209,40	R$ 337.675,20

3.4. **Todos os itens a serem fornecidos neste termo de referência deverão ser do mesmo FABRICANTE e compatíveis com as licenças e equipamentos atualmente em uso, compondo uma solução única**, assegurando a compatibilidade funcional de todos os recursos, conforme disposto no inciso I, artigo 32 da lei 13.303 de 30 de junho de 2016 que regulamenta o art. 37, inciso XXI, da Constituição Federal e institui as normas para licitações e contratos da administração pública;

3.5. **Todos os equipamentos fornecidos deverão ser novos, de primeiro uso e estar em linha de fabricação na data de abertura das propostas** o que deve ser comprovado por documento do **FABRICANTE**, com firma reconhecida e escrito especificamente para este Edital.

3.6. **Nenhum dos modelos ofertados poderá estar listado no site do FABRICANTE como end-of-life (fim de vida) e end-of-sale (fim de vendas)**.

4. CLÁUSULA QUARTA - LOCAL E PRAZO DA ENTREGA DOS PRODUTOS E SERVIÇOS

4.1. Os produtos e serviços objeto deste Termo será executado no prédio Sede da **PRODEPA**, localizado na Rodovia Augusto Montenegro, KM 10, Icoaraci, na cidade de Belém (**PA**).

4.2. O prazo máximo para a entrega dos itens pela CONTRATADA será de **até 90 (noventa) dias corridos**, contados a partir da data de solicitação.

4.3. A **PRODEPA** tem **até 30 (trinta) dias corridos** para emitir o Termo de Aceite Definitivo após o recebimento dos produtos ou serviços.

4.4. A **PRODEPA** tem **até 15 (quinze) dias corridos** para emitir o ateste da Nota Fiscal a emissão do Termo de Aceite Definitivo

5. CLÁUSULA QUINTA - PREÇO

5.1. O **valor Global da contratação** é de **R$ 337.675,20 (trezentos e trinta e sete mil, seiscentos e setenta e cinco reais e vinte centavos)**, para o **período** de **36 (trinta e seis) meses**.

5.2. Nos valores acima foram considerados na composição do preço do objeto licitado todos os custos, aí incluídos as peças, assessórios e equipamentos de reposição, seguros, fretes, tributos (impostos, contribuições, taxas), encargos previdenciários, trabalhistas e comerciais de qualquer

espécie ou quaisquer outras despesas incidentes, direta ou indiretamente, sobre o referido objeto, inclusive o pagamento do diferencial da alíquota, que é de responsabilidade da PRODEPA, e deverão ter perfeita compatibilidade com os valores unitários e totais apresentados para o mesmo. Deverão ainda ser considerados todos os serviços, peças, assessórios e equipamentos de reposição que, embora não mencionados, sejam necessários para a perfeita e integral execução do serviço.

6. CLÁUSULA SEXTA - DOTAÇÃO ORÇAMENTÁRIA

6.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da PRODEPA, para o exercício de 2025, na classificação abaixo:

23.126.1508.2251	MANUTENÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – TIC
01.501.000061	RECURSO PRÓPRIO
449052	EQUIPAMENTO OU MATERIAL PERMANENTE

23.572.1490.2226	AMPLIAÇÃO E MODERNIZAÇÃO DA REDE DE TELECOMUNICAÇÃO
01.501.000061	RECURSO PRÓPRIO
449052	EQUIPAMENTO OU MATERIAL PERMANENTE

7. CLÁUSULA SÉTIMA - REAJUSTE

7.1. Os preços orçados são fixos e irreajustáveis pelo prazo de 12 (doze) meses, contado da data limite para apresentação das propostas, de acordo com o Art. 170 do RILC da PRODEPA.

7.2. Após o interregno de 12 (doze) meses, os preços iniciais poderão ser reajustados com base em índice oficial compatível com o segmento econômico em que esteja inserido o objeto da contratação — na falta de qualquer índice setorial, será adotado o menor dos índices oficiais calculados e divulgados pelo IBGE —, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

7.4. O reajuste se restringirá ao valor do saldo contratual existente na data em que aquele for devido.

7.5. O reajuste será realizado de ofício pelo CONTRATANTE mediante a aplicação do índice de correção monetária mencionado na Cláusula 7.2 na base de cálculo do item 7.4.

7.6. O reajuste será automático e independerá de requerimento da CONTRATADA.

7.7. O reajuste será realizado por simples apostila.

7.8. No caso de atraso ou não divulgação do índice de reajuste, o contratante utilizará a sua última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

7.9. A repactuação de preços, como espécie de reajuste contratual, poderá ser utilizada nas contratações de serviços continuados com dedicação exclusiva de mão de obra, respeitadas as regras referentes aos reajustes de forma geral, desde que prevista no contrato.

7.10. Para fins de repactuação, o interregno mínimo de 12 (doze) meses é contado a partir da data do acordo, convenção ou dissídio coletivo de trabalho ou equivalente, vigente à época da apresentação da proposta.

7.11. A repactuação poderá ser dividida em tantas parcelas quanto forem necessárias e realizada em momentos distintos, para discutir a variação de custos que tenham sua anualidade resultante em datas diferenciadas, tais como nos casos em que a contratação envolver mais de uma categoria profissional, com datas-bases diversas.

7.12. O contrato poderá prever repactuação apenas da parcela contratual referente aos custos decorrentes de mão de obra, aplicando-se o reajuste por índices oficiais, à parcela contratual referente aos demais insumos, respeitadas as periodicidades anuais com datas-bases distintas.

8. CLÁUSULA OITAVA - PAGAMENTO

8.1. O pagamento será realizado **no prazo de até 30 (trinta) dias**, contado do recebimento da nota fiscal ou fatura atestada pelo fiscal do contrato, acompanhado das certidões de regularidade fiscal, através de Ordem Bancária Banco – **OBB** ou de Ordem Bancária Pagamento – **OBP**, de acordo com o art. 6º, inciso II, da **IN SEFA** n.º 18/08, de 21/05/08.

8.2. **O pagamento será realizado em uma única parcela, para os produtos ou serviços de entrega única e imediata**, após a emissão do Termo de Aceite Definitivo dos mesmos.

8.3. **Para o serviço técnico especializado descrito no Item 15, o pagamento será realizado mensalmente**, após o atesto da fiscalização.

8.4. 8.2 O pagamento será efetuado por ordem bancária para conta de titularidade da contratado, cujos dados são:

BANCO	BANCO DO BRASIL
AGÊNCIA	3382-0
CONTA	6734-2

8.5. Havendo erro na apresentação da nota fiscal, fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que o **CONTRATADO** adote as medidas saneadoras pertinentes.

8.5.1. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus ao **CONTRATANTE**.

8.6. Será considerada data do efetivo pagamento a que constar da ordem bancária emitida para quitação da nota fiscal ou fatura.

8.7. A nota fiscal ou fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal do **CONTRATADO**, constatada por meio de consulta "on line" ao Sistema de Cadastramento Unificado de Fornecedores (**SICAF**) ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação física listada no art. 54 do **RILC**.

8.8. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao **SICAF** para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, a que se refere o item 16.3 deste Termo de Referência.

8.9. Constatando-se, junto ao SICAF, a situação de irregularidade do CONTRATADO, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CONTRATANTE.

8.10. Não havendo regularização ou sendo a defesa considerada improcedente, o CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do CONTRATADO, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários a garantir o recebimento de seus créditos.

8.11. Persistindo a irregularidade, o CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos de processo administrativo instaurado para esse fim, assegurando-se ao CONTRATADO a ampla defesa e contraditório.

8.12. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente até que se decida pela rescisão do Contrato, caso o CONTRATADO não regularize sua situação junto ao SICAF.

8.13. Será rescindido o Contrato em execução com CONTRATADO inadimplente no SICAF, salvo por motivo de economicidade, segurança estadual ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela autoridade máxima do CONTRATANTE.

8.14. Por ocasião do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.15. O CONTRATADO, regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8.16. O CONTRATADO deverá pagar, como responsável único, todos os encargos trabalhistas, fiscais e comerciais, que incidam ou venham a incidir, direta ou indiretamente, sobre o objeto do contrato, podendo a PRODEPA, a qualquer momento, exigir da contratada a comprovação de sua regularidade de acordo com o Art. 163. §1º, §2º E §3º da RILC da PRODEPA.

8.17. Deverão constar nas notas fiscais, obrigatoriamente, o número do contrato, além da discriminação da parcela relativa ao evento do faturamento (medição), se for o caso.

8.18. Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido, de alguma forma, para tanto, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \qquad I = \frac{(6 / 100)}{}$$

I = 0,00016438

TX = Percentual da taxa anual = 6%

9. CLÁUSULA NONA – GARANTIA DE CUMPRIMENTO CONTRATUAL

9.1. Para garantia do fiel e perfeito cumprimento das obrigações do futuro contrato, a **CONTRATADA** deverá apresentar à **PRODEPA**, no **prazo de até 15 (quinze) dias após a assinatura do contrato**, qualquer uma das garantias abaixo discriminadas, no valor equivalente a **5% (cinco por cento) sobre o valor do contrato**, atualizável nas mesmas condições daqueles, conforme o artigo 172 do **RILC** da **PRODEPA**

9.1.1. **Caução em dinheiro ou em títulos da dívida pública**, devendo estes ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda

9.1.2. **Fiança bancária**;

9.1.3. **Seguro garantia** feito junto à entidade com situação regular no mercado de seguros do Brasil.

9.2. A garantia em dinheiro deverá ser efetuada em favor da **CONTRATANTE**, depositada no Banco do Estado do Pará – **BANPARÁ**, Agência 15, conta corrente nº 188.000-4, com correção monetária.

9.3. Caso a **CONTRATADA** não apresente a garantia contratual no prazo acima, poderá ser-lhe imputada multa, nos termos do item 12.2.2, subitem 12.2.2.4 deste contrato.

9.3.1. Se a garantia contratual não for apresentada no **prazo de até 30 (trinta) dias após a assinatura do contrato**, este poderá ser **rescindindo unilateralmente pela PRODEPA**.

9.4. Na hipótese de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

9.5. Caso ocorra a situação prevista, a **CONTRATADA** terá até **30 (trinta) dias** para apresentar o reforço da garantia, sob pena de rescisão do contrato.

9.6. Ocorrendo o vencimento da garantia antes do encerramento das obrigações contratuais, a **CONTRATADA** deverá providenciar, às suas expensas, a respectiva renovação, sob pena de rescisão do contrato.

9.7. A **PRODEPA** poderá deduzir da garantia contratual multas e penalidades previstas no contrato, bem como o valor dos prejuízos que lhe forem causados.

9.8. Rescindido o contrato por culpa exclusiva da **CONTRATADA**, a garantia contratual será executada em favor da **PRODEPA**.

9.9. A garantia prestada será devolvida após o encerramento da vigência do contrato (Art. 70, §4º da Lei nº 13.303/16), mediante solicitação expressa e por escrito da **CONTRATADA**, **deduzida de eventuais multas ou débitos pendentes**.

9.10. A garantia prestada para execução do contrato não desobriga a **CONTRATADA** a apresentar a garantia dos serviços prestados, dos equipamentos, das peças, materiais e demais componentes de reposição empregados, conforme estabelecido no Termo de Referência.

10. CLÁUSULA DÉCIMA – OBRIGAÇÕES DAS PARTES

10.1. O **CONTRATANTE** tem a obrigação de:

10.1.1. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com este contrato, Termo de Referência e anexos.

10.1.2. Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações contratuais, inclusive permitir acesso aos profissionais ou representantes da CONTRATADA às dependências, aos equipamentos e aos sistemas de informação do CONTRATANTE relacionados à execução do(s) serviço(s), mas com controle e supervisão das áreas técnicas do CONTRATANTE;

10.1.3. Verificar, detalhadamente e no prazo fixado, a conformidade dos serviços executados pela CONTRATADA, de acordo com as especificações constantes do Edital e da Proposta.

10.1.4. Permitir o acesso, quando se fizer necessário, dos colaboradores da CONTRATADA, devidamente credenciados, às dependências das unidades da PRODEPA, aos dados e demais informações necessárias ao desempenho das atividades previstas no Termo de Referência, ressalvados os casos de matéria sigilosa.

10.1.5. Prestar informações referentes ao contrato sempre que solicitadas pela CONTRATADA.

10.1.6. Executar testes de aceitação a seu exclusivo critério.

10.1.7. Comunicar oficialmente a CONTRATADA qualquer falha verificada no cumprimento do Contrato.

10.1.8. Analisar se os níveis de serviço exigido e indicadores estão sendo alcançados;

10.1.9. Comunicar a CONTRATADA, por escrito, sobre as imperfeições, falhas ou irregularidades verificadas no serviço fornecido, para que seja substituído, reparado ou corrigido.

10.1.10. Exercer a fiscalização e gerenciamento da execução do objeto contratual, através de preposto(s) especialmente designado(s) para este fim e visando o seu exclusivo interesse, sem prejuízo, redução ou exclusão da responsabilidade da CONTRATADA, inclusive perante terceiros da CONTRATADA.

10.1.11. Efetuar o pagamento a CONTRATADA do valor pactuado, no prazo e forma estabelecidos neste Termo de Referência e seus anexos.

10.1.12. Aplicar ao contratado as sanções decorrentes da inexecução total ou parcial do contrato.

10.1.13. Observar para que, durante a vigência do contrato, sejam mantidas todas as condições de habilitação e qualificação exigidas na licitação, bem assim, a compatibilidade com as obrigações assumidas;

10.1.14. Decidir sobre as solicitações e reclamações relacionadas à execução do contrato, ressalvados os requerimentos meramente protelatórios, manifestamente impertinentes ou de nenhum interesse à boa execução do ajuste.

10.1.15. A PRODEPA não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, seus empregados, prepostos ou subordinados.

10.2. A CONTRATADA tem a obrigação de:

10.2.1. Cumprir todas as obrigações constantes deste contrato, seus anexos e proposta, assumindo exclusivamente os riscos e as despesas decorrentes da boa e perfeita execução do objeto contratado.

10.2.2. Designar, por escrito, o funcionário responsável para resolução de eventuais ocorrências durante a execução deste contrato, relativas à assistência técnica dos equipamentos e/ou dos bens adquiridos.

10.2.3. Manter preposto aceito pelo CONTRATANTE no local da prestação do serviço para o representar na execução do contrato.

10.2.4. Responsabilizar-se, integralmente, pelos serviços contratados nos termos da legislação vigente.

10.2.5. Manter as condições de garantia dispostas ne contrato e no Termo de Referência;

10.2.6. Detalhar e repassar o conhecimento técnico utilizado na execução dos serviços, quando solicitado pelo CONTRATANTE.

10.2.7. Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam à Política de Segurança da Informação da CONTRATANTE.

10.2.8. Encaminhar mensalmente a PRODEPA as notas fiscais dos serviços prestados;

10.2.9. A indicação do preposto da CONTRATADA ou a sua manutenção poderá ser recusada pelo CONTRATANTE mediante justificativa, devendo o contratado designar outro para o exercício da atividade.

10.2.10. Responsabilizar-se pelos vícios e danos decorrentes da execução dos serviços, de acordo com os artigos 12, 13 e 17 a 27 do Código de Defesa do Consumidor (Lei nº 8.078, de 1990).

10.2.11. Utilizar somente pessoal protegido conforme a legislação vigente do Ministério do Trabalho e fazer com que seus colaboradores, sob sua responsabilidade, usem EPI's completos, respeitas as normas relativas à segurança, higiene e medicina do trabalho.

10.2.12. Planejar, conduzir e executar os serviços dentro das Normas de Segurança do Trabalho, Saúde e Meio Ambiente, vigentes e exigíveis por lei.

10.2.13. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior e prestar esclarecimentos ou informações por eles solicitados.

10.2.14. Alocar os empregados em número compatível para o cumprimento deste contrato e com a habilitação e conhecimento adequados para a execução do serviço, **fornecendo os materiais, equipamentos, ferramentas e utensílios necessários** para tanto, cuja quantidade, qualidade e tecnologia deverão atender às recomendações dos órgãos de regulação responsáveis e à legislação aplicável.

10.2.15. Substituir por outro profissional de qualificação igual ou superior qualquer um dos seus profissionais cuja qualificação, atuação, permanência ou comportamento decorrente da execução do objeto for julgado prejudicial, inconveniente ou insatisfatório à disciplina da CONTRATANTE ou ao interesse do serviço público, sempre que exigido;

10.2.16. No prazo fixado pelo fiscal do contrato, reparar, corrigir ou refazer às suas expensas o serviço no qual se verificar vícios, defeitos ou incorreções resultantes de sua má execução contratual ou dos materiais empregados.

10.2.17. Durante a vigência do contrato, não contratar cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o 3º grau, de dirigente do contratante ou de agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato.

10.2.18. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato e obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao CONTRATANTE.

10.2.19. Cumprir todas as normas internas e procedimentos administrativos da CONTRATANTE.

10.2.20. Em hipótese alguma, o desconhecimento das condições operacionais poderá ser alegado como justificativa para inexecução ou execução irregular dos serviços a serem prestados;

10.2.21. Arcar com os custos de transportes e seguro dos equipamentos a serem utilizados nas manutenções corretivas, inclusive os de propriedade da CONTRATANTE, que forem entregues a CONTRATADA para a utilização nos serviços de manutenção.

10.2.22. Todas as despesas com alimentação, hospedagem, transportes, leis sociais, seguros, licenças, taxas e impostos correrão por conta da CONTRATADA.

10.2.23. No caso de troca ou reposição dos objetos, a CONTRATADA assumirá também a responsabilidade pelos custos de transporte, carga, descarga e instalação.

10.2.24. Cumprir as posturas do Município e as disposições legais estaduais e federais que interfiram na execução do objeto.

10.2.25. Manter, durante toda a execução do objeto, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas neste contrato e no Termo de Referência.

10.2.26. Participar, dentro do período compreendido entre a assinatura do contrato e o início da prestação dos serviços, de reunião de alinhamento de expectativas contratuais com a equipe da PRODEPA.

10.2.27. Reportar à PRODEPA, imediatamente, quaisquer anormalidades, erros ou irregularidades que possam comprometer a execução dos serviços e o bom andamento das atividades.

10.2.28. A CONTRATADA deverá manter sigilo em relação aos dados, informações ou documentos que tomar conhecimento em decorrência da prestação dos serviços objeto desta contratação, bem como se submeter às orientações e normas internas de segurança da informação vigentes, devendo orientar seus empregados e/ou prepostos nesse sentido sob pena de responsabilidade civil, penal e administrativa.

10.2.29. Obedecer, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de TI da PRODEPA.

10.2.30. Pagar, como responsável único, todos os encargos trabalhistas, fiscais e comerciais, que incidam ou venham a incidir, direta ou indiretamente, sobre os serviços contratados, podendo a PRODEPA, a qualquer momento, exigir da contratada a comprovação de sua regularidade de acordo com o Art. 163. §1º, §2º E §3º da RILC PRODEPA.

10.2.31. Prestar todo esclarecimento ou informação solicitada pelo CONTRATANTE ou por seus prepostos, garantindo-lhes, a qualquer tempo, o acesso ao local dos trabalhos e aos documentos relativos à execução do serviço.

10.2.32. Por determinação do CONTRATANTE, paralisar a atividade que não esteja sendo bem executada ou que ponha em risco a segurança das pessoas ou seus bens.

10.2.33. Durante a vigência do contrato, promover a guarda, manutenção e vigilância de materiais,

ferramentas e tudo o que for necessário à execução do serviço.

10.2.34. Conduzir os trabalhos observando às normas da legislação aplicável e às determinações dos Poderes Públicos, mantendo o local dos serviços limpo e nas melhores condições de segurança, higiene e disciplina.

10.2.35. Submeter previamente e por escrito ao CONTRATANTE qualquer mudança nos métodos executivos especificados no memorial descritivo ou documento similar para sua análise e aprovação.

10.2.36. Não permitir:

a) o trabalho de pessoa menor de 16 anos no objeto deste contrato, exceto na condição de aprendiz para os maiores de 14 anos; e

b) a utilização do trabalho da pessoa menor de 18 anos em trabalho noturno, perigoso ou insalubre, em qualquer hipótese.

10.2.37. Cumprir durante todo o período de execução do contrato a reserva de cargos para pessoa com deficiência, reabilitado da Previdência Social, aprendiz e outras reservas de cargos previstas na legislação.

10.2.38. Comprovar o cumprimento da alínea acima no prazo fixado pelo fiscal do contrato, indicando os empregados que preencheram as referidas vagas.

10.2.39. Manter seus profissionais, nas dependências da CONTRATANTE, adequadamente trajados e identificados com uso permanente de crachá, com foto e nome visível.

10.2.40. A CONTRATADA obriga-se a substituir, às suas expensas, no total ou em parte, os bens que apresentarem qualquer irregularidade.

10.2.41. Em nenhuma hipótese poderá a CONTRATADA veicular publicidade acerca do serviço a que se refere o presente objeto, salvo com a devida autorização do CONTRATANTE.

10.2.42. É terminantemente vedada a contratação de servidor pertencente ao quadro de pessoal do CONTRATANTE.

10.2.43. Não reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer informações de que tenha tomado conhecimento em razão da execução dos serviços objeto deste Termo de Referência sem o consentimento, por escrito, do CONTRATANTE.

10.2.44. Arcar com o ônus decorrente de eventual equívoco no dimensionamento do quantitativo de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos do art. 81, VI, da Lei Federal nº 13.303/16.

11. CLÁUSULA DÉCIMA PRIMEIRA – RESPONSABILIDADE POR DANOS

11.1. A responsabilidade pelos danos causados por ato do contratado, de seus empregados, prepostos ou subordinado, é exclusivamente da CONTRATADA.

11.2. A responsabilidade pelos compromissos assumidos pela CONTRATADA com terceiros é exclusivamente sua.

11.3. O CONTRATANTE não responderá pelos compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução deste contrato, ou por qualquer dano causado por ato

da **CONTRATADA**, de seus empregados, prepostos ou subordinados.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMNISTRATIVAS

12.1. Comete infração administrativa, nos termos da Lei Estadual nº. 6.474/2002 c/c Lei nº 13.303/2016 e o **RILC** da **PRODEPA**, a **CONTRATADA** que:

12.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

12.1.2. ensejar o retardamento da execução do serviço;

12.1.3. falhar ou fraudar na execução do contrato;

12.1.4. comportar-se de modo inidôneo;

12.1.5. cometer fraude fiscal.

12.2. Pela inexecução total ou parcial do objeto do contrato, a **PRODEPA** pode aplicar ao **CONTRATADO** as seguintes sanções:

12.2.1. **Advertência**, aplicada por meio de notificação por escrito, estabelecendo-se prazo razoável para o adimplemento da obrigação pendente;

12.2.2. **Multa** de **10% (dez por cento) sobre o valor do contrato**, pela recusa injustificada em celebrar o contrato;

12.2.3. **Multa** de **0,5% (zero vírgula cinco por cento) sobre o valor correspondente ao item afetado**, por dia de atraso injustificado durante a execução dos produtos ou serviço, **limitado a 10% (dez por cento)** correspondente ao item afetado;

12.2.4. **Multa** de **0,2% (zero vírgula dois por cento) sobre o valor correspondente ao item afetado**, por cada dia de atraso injustificado em que o suporte estiver indisponível para atendimento, **limitado a 10% (dez por cento)** correspondente ao item afetado;

12.2.5. **Multa** de **0,2% (zero vírgula dois por cento) sobre o valor do contrato por cada dia em que houver a ausência de profissional** no quadro de funcionários da **CONTRATADA** no perfil profissional **limitado a 10% (dez por cento)** do valor do contrato;

12.2.6. **Multa** de **0,1% (zero vírgula um por cento) sobre o valor correspondente ao item afetado**, por cada hora de atraso injustificado decorridas após o prazo máximo referente ao suporte estipulado no item **Acordo de Nível Serviço** consignado no Termo de Referência, limitado a **10 (dez por cento)** correspondente ao item afetado.

12.2.6.1. Em relação aos prazos estipulados pelo **item que trata do Serviços de Suporte Técnico Especializado** poderá ensejar **desconto sobre o valor mensal devido**, conforme quadro abaixo:

Severidade dos Chamados	Percentual de atendimento dentro do ANS	Penalidade (% de glosa)
1 e 2	Acima de 95%	Não há
	Entre 90% e 94,9%	10%
	Entre 85% e 89,9%	15%
	Abaixo de 84,9%	20%
3 e 4	Acima de 95%	Não há

	Entre 90% e 94,9%	5%
	Entre 85% e 89,9%	7,5%
	Abaixo de 84,9%	10%

12.2.7. **Suspensão do direito de licitar e contratar** com a **PRODEPA** por prazo não superior a 02 (dois) anos, quando a **CONTRATADA** permanecer no descumprimento das obrigações contratuais;

12.3. As sanções tratadas serão aplicadas pela **CONTRATANTE**.

12.4. No caso de atraso injustificado na execução do objeto licitado por **período superior a 30 (trinta) dias**, poderá ensejar a **rescisão do contrato**.

12.5. As penalidades serão aplicadas sem prejuízo das demais sanções, administrativas ou penais, previstas na Lei Federal 13.303/2016.

12.6. Em qualquer hipótese de aplicação de sanções, fica assegurada à **CONTRATADA** o direito ao contraditório e a ampla defesa.

12.7. Não será aplicada multa se, justificada e comprovadamente, o inadimplemento de qualquer cláusula contratual advir de caso fortuito, motivo de força maior ou fato do príncipe.

12.8. Caso os serviços prestados ou os equipamentos não correspondam às especificações exigidas no Termo de Referência, a **CONTRATADA** deverá adequá-los àquelas, no prazo estabelecido pela Fiscalização, sob pena de aplicação da penalidade cominada para a hipótese de inexecução total.

12.9. As multas devidas e/ou prejuízos causados à **CONTRATANTE** serão deduzidos dos valores a serem pagos, ou recolhidos em favor da **PRODEPA**, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa do Estado e cobrados judicialmente.

12.9.1. Caso a **PRODEPA** determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.10. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do **CONTRATADO**, a **PRODEPA** poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

12.11. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao **CONTRATADO**, observando-se o procedimento previsto no art. 185 e seguintes do **RILC** da **PRODEPA**, e subsidiariamente na Lei Federal nº 9.784, de 1999, e na Lei Estadual nº 8.972, de 13 de janeiro de 2020.

12.12. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

12.13. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei Federal nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou processo administrativo.

12.14. A personalidade jurídica do CONTRATADO poderá ser desconsiderada quando for utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste contrato ou para provocar confusão patrimonial e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o contratado, observados o contraditório, ampla defesa e a obrigatoriedade de análise jurídica prévia.

12.15. Não serão aplicadas sanções se, justificada e comprovadamente, o inadimplemento de qualquer cláusula contratual advir de caso fortuito, motivo de força maior ou fato do príncipe.

12.16. O valor das multas aplicadas será creditado a favor da PRODEPA, sendo vedado à CONTRATADA qualquer posicionamento que inviabilize a compensação e abatimento, podendo ser o contrato rescindido por tal prática.

12.17. No caso de inadimplemento que resultar em aplicação de multa, o pagamento devido só poderá ser liberado após a apresentação da guia de recolhimento da multa em questão ou mediante o desconto do valor da mesma sobre o total da fatura ou da nota fiscal.

12.18. No caso das multas aplicadas, somadas ou não, ultrapassarem o valor da garantia apresentada neste contrato, deverá a CONTRATADA, sob pena de rescisão contratual, depositar novo valor, no mesmo importe do inicial, no prazo máximo de 30 (trinta) dias, seja qual for a etapa de execução do contrato.

12.19. As sanções previstas nesta cláusula poderão ser aplicadas isolada ou cumulativamente.

12.20. Ao final do processo administrativo punitivo, compete à área de Contratos providenciar o registro da penalidade aplicada no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), Cadastro Nacional de Empresas Punidas (CNEP), Sistema de Cadastramento Unificado de Fornecedores – SICAF e, ainda, no Sistema de Materiais e Serviços – SIMAS.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES DO CONTRATO

13.1. As eventuais alterações contratuais deverão observar o disposto nos arts. 72 e 81 da Lei Federal nº 13.303/2016 e no Regulamento Interno de Licitações e Contratos — RILC — da PRODEPA.

13.2. Os contratos regidos por esta Lei somente poderão ser alterados por acordo entre as partes, vedando-se ajuste que resulte em violação da obrigação de licitar.

13.3. O CONTRATADO poderá aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nas obras, serviços ou compras, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, e, no caso particular de reforma de edifício ou de equipamento, até o limite de 50% (cinquenta por cento) para os seus acréscimos.

13.3.1. Nenhum acréscimo ou supressão poderá exceder os limites acima estabelecidos, salvo as supressões resultantes de acordo celebrado entre os contratantes.

13.4. Os acréscimos ou supressões não podem transfigurar o objeto da contratação.

13.5. Registros que não caracterizem alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, conforme art. 174 do RILC da PRODEPA.

14. CLÁUSULA DÉCIMA QUARTA – EXTINÇÃO DO CONTRATO

14.1. Os contratos firmados pela PRODEPA serão extintos, nas hipóteses previstas nos art. 183 e

184 do RILC:

14.1.1. Com o advento de seu termo, se por prazo certo;

14.1.2. Com a conclusão de seu objeto, quando por escopo;

14.1.3. Antecipadamente, por acordo entre as partes ou por via judicial;

14.1.4. Por Razões de interesse público, de alta relevância e amplo conhecimento, justificados e determinados pela máxima autoridade da PRODEPA e exaradas no processo administrativo a que se refere o contrato;

14.1.5. A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da sua execução ou fornecimento;

14.1.6. Pelo descumprimento de obrigações trabalhistas e/ou não manutenção das condições de habilitação pela CONTRATADA exigidas no processo licitatório, sem prejuízo da aplicação das sanções cabíveis.

14.1.6.1. A PRODEPA poderá conceder prazo razoável para a CONTRATADA regularize suas obrigações trabalhistas e suas condições de habilitação, ou ainda, da apresentação da garantia.

14.1.7. Descumprimento de condições contratuais que tragam danos relevantes para a PRODEPA, tais como a lentidão do seu cumprimento, comprovando a impossibilidade da conclusão dos serviços ou do fornecimento nos prazos estipulados e o desatendimento reiterado de determinações regulares da fiscalização.

14.1.8. O não cumprimento ou o cumprimento irregular de cláusulas contratuais, especificações e prazos, combinados com o cometimento reiterado de faltas na sua execução, gerando má qualidade na execução do objeto contratado, sem prejuízo da aplicação das sanções cabíveis previstas no art. 187 do RILC da PRODEPA.

14.2. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurando o contraditório e ampla defesa nos termos do art. 5º, inciso LV da Constituição Federal.

14.3. Constituem, ainda, motivos para a rescisão do contrato:

14.3.1. A decretação de falência ou instauração de insolvência civil da CONTRATADA.

14.3.2. A dissolução da sociedade da CONTRATADA.

14.3.3. A alteração social ou modificação da finalidade ou da estrutura da CONTRATADA, que, a juízo da PRODEPA, prejudique a execução do contrato.

14.3.4. O termo de rescisão será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso: Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

14.3.5. Relação dos pagamentos já efetuados e ainda devidos;

14.3.6. Indenizações e multas.

15. CLÁUSULA DÉCIMA QUINTA - ALTERAÇÃO SUBJETIVA.

15.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do Contrato; não haja

prejuízo à execução do objeto pactuado; e haja anuência expressa da PRODEPA à continuidade do Contrato.

16. CLÁUSULA DÉCIMA SEXTA – FISCALIZAÇÃO

16.1. Os serviços objeto desta contratação serão fiscalizados pela CONTRATANTE, que para isso indicará 01 (um) preposto com o qual serão estabelecidos todos os contatos durante a execução do contrato.

16.2. A fiscalização e aceite dos serviços dar-se-á após encerramento do chamado junto a CONTRATANTE.

16.3. A fiscalização poderá ocorrer a qualquer momento durante a realização das manutenções corretivas por decisão única e exclusiva da CONTRATANTE.

16.4. Após a conferência dos serviços, se constatado o serviço incompleto, de má qualidade ou divergência daquele ofertado pela CONTRATADA, esta estará obrigada a refazer o serviço sob pena de aplicação das penalidades previstas no contrato, sem que isso implique em novo ônus a CONTRATANTE.

16.5. Nos termos do art. 159, inciso XIV do RILC da PRODEPA, será designado representante do CONTRATANTE para acompanhar e fiscalizar a execução dos serviços, anotando em registro próprio todas as ocorrências relacionadas à execução do Contrato e determinando o que for necessário à regularização de falhas ou defeitos observados.

16.6. A fiscalização de que trata este item não exclui nem reduz a responsabilidade do CONTRATADO, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, a ocorrência desses eventos, não implicará a corresponsabilidade da PRODEPA ou de seus agentes e prepostos, em conformidade com o disposto no art. 163, §2º do RILC.

16.7. O representante da PRODEPA anotará em registro próprio todas as ocorrências relacionadas à execução do Contrato, indicando dia, mês e ano, bem como o nome dos empregados ou prepostos eventualmente envolvidos, determinando o que for necessário à regularização de falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente, para as providências cabíveis.

17. CLÁUSULA DÉCIMA SÉTIMA – INTERPRETAÇÃO

17.1. As dúvidas interpretativas sobre as cláusulas deste contrato deverão ser suscitadas ao CONTRATANTE e serão decididas por ele, de acordo com a Lei Federal nº 13.303/16, seus regulamentos, Lei Estadual n° 8.972/20, RILC da PRODEPA e observando a jurisprudência dos Tribunais sobre o assunto.

18. CLÁUSULA DÉCIMA OITVA– TRATAMENTO ADEQUADO DOS CONFLITOS DE INTERESSE

18.1. Observado o disposto na Cláusula 17, permanecendo o conflito de interesse, as partes se comprometem a submeter a disputa preferencialmente à Câmara de negociação, conciliação, mediação e arbitragem da administração pública estadual para dirimir os conflitos decorrentes deste contrato de maneira consensual, conforme Lei Complementar Estadual n° 121/19.

19. CLÁUSULA DÉCIMA NONA – DIVULGAÇÃO E PUBLICAÇÃO

19.1. O presente contrato será divulgado no Portal Nacional de Contratações Públicas (PNCP) em

até 20 dias úteis e o publicará no Diário Oficial do Estado em forma de extrato, no prazo de até 30 (trinta) dias, contados a partir de sua assinatura, de acordo com o art. 157 do RILC da CONTRATANTE.

20. CLÁUSULA VIGÉSIMA – VIGÊNCIA

20.1. O Contrato terá a vigência de 36(trinta e seis) meses, com início em XX/07/2025 e término em XX/XX/20XX, prorrogável até o limite de 60 (sessenta) meses, mediante justificativa, conforme art. 71, inciso I e II, § único, da Lei nº 13.303, de 2016.

20.2. Antes da prorrogação da vigência do contrato, o contratante deverá verificar a regularidade fiscal do contratado, consultar o CEIS e o CNEP, emitir as certidões negativas de inidoneidade, de impedimento e de débitos trabalhistas e juntá-las ao respectivo processo.

21. CLÁUSULA VIGÉSIMA PRIMEIRA – FORO

21.1. As partes elegem o Foro da cidade de Belém, Estado do Pará, para dirimir quaisquer litígios oriundos do presente contrato, excluindo-se qualquer outro, por mais privilegiado que seja observado o disposto na Cláusula 18.

Belém - Pará, de julho de 2025.

CARLOS EDILSON DE ALMEIDA MANESCHY:06616690253

Assinado de forma digital por CARLOS EDILSON DE ALMEIDA MANESCHY:06616690253

CARLOS EDILSON DE ALMEIDA MANESCHY
Presidente da PRODEPA

Documento assinado digitalmente
gov.br
MURILO ROSSETTO
Data: 29/07/2025 17:01:30-0300
Verifique em https://validar.iti.gov.br

MURILO ROSSETTO
Representante Legal

TESTEMUNHAS:

1._____ 2. _____

Nome Nome

CPF/MF: CPF/MF

ANEXO I
TERMO DE REFERÊNCIA

1. OBJETO

1.1. Registro de Preço para **AQUISIÇÃO DE SOLUÇÃO FIREWALL**, com treinamento e serviços técnicos especializados com instalação, configuração, operação assistida e continuada, conforme condições, quantidades e exigências estabelecidas neste instrumento.

LOTE	ITEM	DESCRIÇÃO	UND	QTDE
ÚNICO	1	Solução de Firewall de Próxima Geração (NGFW) – TIPO 01	Unid.	02
	2	Solução de Firewall de Próxima Geração (NGFW) – TIPO 02	Unid.	02
	3	Solução de Firewall de Próxima Geração (NGFW) – TIPO 03	Unid.	350
	4	Gerenciamento Centralizado de Logs e Relatoria – TIPO GERENCIA	Unid.	04
	5	Gerenciamento Centralizado de Logs e Relatoria – TIPO LOGS	Unid.	03
	6	Transceiver SFP+ 10GBase-SR	Unid.	24
	7	Transceiver SFP+ 10GBase-LR	Unid.	24
	8	Transceiver SFP 1000Base-SX	Unid.	300
	9	Transceiver SFP 1000Base-LX	Unid.	50
	10	Transceiver QSFP+ 40GBase-SR4	Unid.	16
	11	Transceiver QSFP28 100GBase-SR4	Unid.	08
	12	Serviço de Implantação (Instalação, Migração e Atualização) da Solução – TIPO 01 e 02	Unid.	04
	13	Serviço de Implantação/Instalação de *Firewall* – Tipo 03	Unid.	350
	14	Treinamento da Solução	Turma	04
	15	Serviço técnico especializado para operação continua e monitoramento, incluindo suporte preventivo e corretivo para Solução de Firewall	Mês	36

1.2. Todos os itens a serem fornecidos neste termo de referência deverão ser do mesmo FABRICANTE e compatíveis com as licenças e equipamentos atualmente em uso, compondo uma solução única, assegurando a compatibilidade funcional de todos os recursos, conforme disposto no inciso I, artigo 32 da lei 13.303 de 30 de junho de 2016 que regulamenta o art. 37, inciso XXI, da Constituição Federal e institui as normas para licitações e contratos da administração pública;

1.3. Todos os equipamentos fornecidos deverão ser novos, de primeiro uso e estar em linha de fabricação na data de abertura das propostas o que deve ser comprovado por documento do FABRICANTE, com firma reconhecida e escrito especificamente para este Edital.

1.4. Nenhum dos modelos ofertados poderá estar listado no site do FABRICANTE como end-of-life (fim de vida) e end-of-sale (fim de vendas);

1.5. Em caso de discordância entre as especificações descritas no sistema eletrônico (Compras.gov) com as constantes deste termo de referência, prevalecerão as deste último.

2. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

2.1. A Empresa de Tecnologia da Informação e Comunicação do Estado do Pará (PRODEPA) é a empresa responsável pela área de Tecnologia no âmbito do Poder Executivo do Estado do Pará, atuando como provedor de serviços para diversos órgãos do Governo Estadual, tanto na capital quanto no interior. Desta forma, busca em suas contratações, novas tecnologias para beneficiar o cidadão paraense por meio do atendimento das diversas necessidades de seus clientes a fim de oferecer serviços de qualidade, compatíveis com a demanda atual e futura.

2.2. Para desempenhar seu papel institucional, a PRODEPA possui um grande parque tecnológico composto de vários ativos, rede e sistemas que exigem da Empresa, a adoção de práticas de segurança visando resguardar seu ambiente tecnológico e preservar dados armazenados e sustentados em sistemas.

2.3. A necessidade pode ser descrita como sendo a proteção do parque tecnológico (servidores e ativos de rede) e dados, mediante solução de gestão de vulnerabilidades, com vistas ao monitoramento e aperfeiçoamento dos serviços prestados pela PRODEPA.

2.4. A PRODEPA com base em seu planejamento estratégico, objetiva o aprimoramento dos processos internos com a adequação da capacidade de Tecnologia da Informação ao crescimento do negócio, adequação da infraestrutura de TI e de telecomunicações e, assim, garantir níveis de serviços de segurança da informação e patrimonial satisfatórios, mantendo um alto grau de desempenho, gerenciamento, disponibilidade, robustez e segurança.

2.5. Desde 2022, o Pará integra lista de capitais que já aderiram à rede Gov.br, o que significa que, junto com outros municípios e estados, vai ampliar a oferta de serviços públicos em meios digitais. A fim de fomentar a transformação digital e trazer aos cidadãos paraenses facilidade e segurança no acesso aos serviços públicos, o Governo do Pará fechou parceria com a Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia e aderiu ao gov.br, uma rede colaborativa que promove o intercâmbio, a articulação e a criação de iniciativas inovadoras referentes à transformação digital no setor público. O objetivo é migrar serviços para o meio digital, integrando estados e municípios na busca por um governo 100% digital.

2.6. O Governo do Estado já vem trabalhando ao longo dos anos nessa integração de alguns serviços com o gov.br, o que significa dizer que o cidadão vai poder acessar estes serviços através de um login único já cadastrado em aplicativos como, por exemplo, Conecte SUS, E-título e CNH digital. Com tudo isso, busca promover uma transformação digital em todo o estado, o que eleva a necessidade de se investir em recursos tecnológicos voltados à segurança da informação. Não basta apenas migrar serviços sem se preocupar em investir em recursos de segurança capazes de impedir ataques, sequestros de dados, invasões e exposição de dados. O segmento de segurança da informação é amplo e existem várias ferramentas e soluções para as mais diversas possibilidades e diante desse cenário, observa-se uma aceleração para esse meio digital e a segurança vem sendo deixada de lado.

2.7. A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que entrou em vigor em setembro de 2020 e tem como objetivo regulamentar o tratamento de dados pessoais por parte de organizações, sejam elas públicas ou privadas. No caso de órgãos públicos, a LGPD impõe uma série de requisitos e responsabilidades, como por exemplo, a adoção de medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra acessos não

autorizados, perda, alteração, divulgação ou destruição.

2.8. Há, ainda, a obrigatoriedade de se notificar incidentes, quando podem comprometer os dados pessoais, os órgãos públicos devem notificar a Autoridade Nacional de Proteção de Dados (ANPD) e, em alguns casos, os titulares afetados, entretanto não basta estruturar e seguir a lei quanto às ações corretivas, quando na verdade, as principais são todas preventivas.

2.9. A PRODEPA utiliza equipamentos de firewall de próxima geração para manter a segurança computacional da rede do Estado com técnicas avançadas de prevenção de intrusão e análise de malwares, todas realizadas de modo automatizado pela própria solução, sendo este um requisito primordial nas solicitações de fornecimento de soluções para o Estado que requer um nível elevado de segurança.

2.10. Com o acelerado crescimento da rede do Estado ao longo destes anos, os equipamentos atuais encontram-se perto da sua capacidade limite sendo necessária a expansão dos mesmos de modo a comportar a necessidade atual e futura sem comprometer o bom funcionamento da rede, inclusive com o fornecimento de constantes expansões que são necessárias para o funcionamento das aplicações requeridas, sejam elas disponibilizadas pelo próprio Estado ou pela Internet. É importante mencionar grandes eventos que já estão previstos para o futuro como a COP30 que ocorrerá em 2025, conforme fundamentado no PAE 2023/1277776, sendo necessário expandir para garantir a conectividade necessária ao evento, uma vez que a infraestrutura atual já se mostrou insuficiente para tal.

2.11. Diante dos riscos citados, surge a indispensável necessidade de se proteger o ambiente e todos os seus dados, gerindo vulnerabilidades, monitorando e permitindo o aperfeiçoamento dos serviços prestados, com vistas à sustentação de seus negócios.

2.12. Como a PRODEPA possui possibilidade em oferecer serviços de segurança ao Estado, fica notória a grande oportunidade de preencher esta lacuna, disponibilizando produtos e serviços personalizados, que atendam essa demanda desses órgãos. Desta forma, a PRODEPA pode atender demandas próprias ao mesmo tempo em que apoia entes públicos na gestão de segurança de seus parques tecnológicos (servidores e ativos de rede) e dados, mediante gestão de vulnerabilidades, mitigando o risco no Estado.

2.13. Os itens foram agrupados em lote único de modo que sejam do mesmo fornecedor com a finalidade de assegurar a compatibilidade entre seus componentes, compondo assim uma solução única, assegurando a compatibilidade funcional de todos os recursos, evitando os riscos de conflitos de propriedade intelectual ao utilizar produtos de fornecedores divergentes e reduzindo o potencial de gerar prejuízos à PRODEPA. Desta forma, justifica-se a utilização de lote único para assegurar melhor competividade sem prejuízo à compatibilidade técnica dos produtos na solução preconizada neste Termo de Referência.

2.14. Considerando o término iminente do contrato vigente e a expiração da assinatura de suporte e atualização no próximo dia 24/04/2024, é essencial a manutenção do perfeito funcionamento da solução. Caso a PRODEPA esteja impedida de atualizar seus sistemas, por falta de licenciamento compatível, uma grave falha de segurança poderá ocorrer nos serviços de TIC do Estado, pois os referidos dispositivos não terão acesso as atualizações de segurança disponibilizada pelo fabricante e não oferecerão proteção contra novas ameaças em razão de ausência de suporte/atualização, que em caso de falha ou invasão, poderá deixar o Estado do Pará sem a possibilidade de diversos serviços de TIC acarretando em prejuízos incomensuráveis.

2.15. Por fim, diante do exposto, reconhecendo a necessidade de aprimorar a segurança, seus serviços e a tecnologia utilizada, alinhado ao planejamento estratégico da PRODEPA, torna-se

necessário realizar aquisição com as especificidades dispostas consoantes a este Termo de Referência.

3. NATUREZA DO SERVIÇO

3.1. O objeto do presente certame **enquadra-se como serviço de natureza COMUM e CONTÍNUA**, conforme definido no parágrafo único do art. 1º da Lei Federal nº 10.520/2002 c/c §1º do art. 1º da Lei Estadual nº 6.474/2002, uma vez que os padrões de desempenho e qualidade estão objetivamente definidos neste Termo de Referência, tendo como base as especificações usuais de mercado.

4. CRITÉRIOS DE SELEÇÃO

4.1. Por se tratar de serviços de natureza comum, sua forma de contratação será mediante licitação na modalidade Pregão Eletrônica, com fundamento no art. 32, inciso IV da Lei nº. 13.303/2016 e art. 78 do **RILC** da **PRODEPA**.

4.2. O critério de julgamento adotado será o **MENOR PREÇO** global do **LOTE**, conforme definido neste edital e seus anexos.

4.3. O orçamento estimado para a contratação é **SIGILOSO**, de acordo com o art. 79 do **RILC** da **PRODEPA**.

4.3.1. O custo estimado da contratação será tornado público apenas e imediatamente após o encerramento do envio de lances.

4.4. A proposta ou o lance vencedor deverá observar os valores unitários e globais máximos fixados (Acórdão nº 1455/2018-TCU-Plenário), ou desconto mínimo exigido, sob pena de desclassificação.

5. REQUISITOS DE HABILITAÇÃO TÉCNICA DA CONTRATADA

5.1. Para fins de **QUALIFICAÇÃO TÉCNICA**, as empresas participantes deverão apresentar os seguintes documentos:

5.1.1. **Comprovar que é representante ou parceiro oficial e credenciado junto ao FABRICANTE** dos produtos ofertados, mediante apresentação de declaração ou documento comprobatório durante a fase de habilitação;

5.1.2. **Apresentação de, no mínimo, 01(um) Atestado de Capacidade Técnica emitido por pessoa jurídica de direito público ou privado**, comprovando que forneceu objetos compatíveis com os objetos desta licitação emitidos em papel timbrado, com assinatura, identificação e telefone do emitente.

5.1.3. **Apresentar DECLARAÇÃO emitida pelo FABRICANTE** ou outro documento que comprove que é revenda autorizada e está apta a comercializar os serviços objetos da licitação indicado neste Termo de Referência;

5.1.4. **Apresentação de, no mínimo, 01(um) Atestado de Capacidade Técnica** emitido por pessoa jurídica de direito público ou privado, comprovando que fornece/forneceu os seguintes:

5.1.4.1. **Solução de Firewall de Próxima Geração (NGFW)** com quantidade **25%** do total registrado;

5.1.4.2. **Solução de Gerenciamento centralizado de Logs e Relatoria** para pelo menos **03 (três)** dispositivos conectados;

5.1.4.3. **Serviços de Implantação de solução de Firewall de Próxima Geração** em cluster de Alta Disponibilidade;

5.1.4.4. **Suporte Técnico Especializado em regime 24x7** pelo período de pelo **menos 12 (doze) meses** ininterruptos;

5.1.4.5. **Treinamento, transferência de conhecimento ou curso ministrado de duração mínima 20 (vinte) horas**;

5.1.5. **Comprovar que possui em seu quadro de colaboradores, um profissional com certificação técnica do FABRICANTE**, para a execução dos serviços.

5.1.5.1. No caso da contratação do próprio **FABRICANTE** para execução dos serviços, deverá ser apresentado esta comprovação no momento da habilitação; ou,

5.1.5.2. **Apresentar declaração de que apresentará o profissional com a certificação técnica do FABIRCANTE no momento da assinatura do contrato**.

5.1.6. **Documento emitido pelo FABRICANTE, com firma reconhecida e específico para este Edital, que todos os equipamentos fornecidos são novos, de primeiro uso e em linha de fabricação** na data de abertura das propostas.

5.2. Todos os itens a serem fornecidos neste termo de referência deverão ser do mesmo FABRICANTE e compatíveis com as licenças e equipamentos atualmente em uso, compondo uma solução única, assegurando a compatibilidade funcional de todos os recursos, conforme disposto no inciso I, artigo 32 da lei 13.303 de 30 de junho de 2016 que regulamenta o art. 37, inciso XXI, da Constituição Federal e institui as normas para licitações e contratos da administração pública;

5.3. **Nenhum dos modelos ofertados poderá estar listado no site do FABRICANTE como** end-of-life (fim de vida) e end-of-sale (fim de vendas).

6. FORMA DE PRESTAÇÃO DO SERVIÇO

6.1. Características Gerais

6.1.1. Os componentes da solução deverão ser do mesmo **FABRICANTE**, de modo a evitar possíveis problemas de compatibilidade entre versões ou tecnologias divergentes;

6.1.2. Todas as versões dos softwares fornecidos deverão estar na última versão estável lançada publicamente.

6.1.3. A garantia das licenças inclui suporte técnico e direito de atualizações de versão pelo período de vigência da mesma.

6.1.4. A garantia de atualização dos produtos deverá disponibilizar upgrades para novas versões e correções dos produtos contratados, desenvolvidos durante o período de vigência do contrato e no catálogo ativo do **FABRICANTE**;

6.1.5. A garantia também inclui correções de eventuais erros ou falhas decorrentes do funcionamento dos softwares componentes da solução, mediante a disponibilização de atualizações corretivas e/ou ajustes de configuração.

6.1.6. A atualização dos produtos deve fornecer upgrades para novas versões (ou patches) publicados durante o período de garantia;

6.1.7. Os quantitativos dos itens definidos no **QUADRO RESUMO** acima são apenas uma previsão, isto é, refletem apenas uma a **estimativa de aquisição**, não implicando, por

conseguinte, em obrigatoriedade da contratação de tais quantidades pela Administração Pública, durante a vigência do Registro de Preços.

6.1.8. Todos os itens são considerados como contratação sob demanda, isto é, não implicam em obrigatoriedade do consumo ou contratação durante a vigência do Registro de Preços e/ou CONTRATO.

6.1.9. As estimativas foram levantadas baseadas nas seguintes premissas:

6.1.9.1. Estrutura e demanda existente hoje no PRODEPA;

6.1.9.2. Perspectiva de crescimento da estrutura e demanda existente;

6.1.9.3. Perspectiva futura da PRODEPA incorporar e/ou atender novas demandas, incluindo demandas de outros órgãos da Administração Pública;

6.1.10. As licenças, referentes aos produtos, devem estar em nome da CONTRATANTE, em modo definitivo, legalizado, não sendo admitidas versões "shareware" ou "trial".

6.2. Em relação as demais características e especificações técnicas dos itens referentes à solução de firewall, incluindo treinamento e serviços técnicos especializados correlatos encontram-se no ANEXO I-A - ESPECIFICAÇÕES TÉCNICAS.

7. LOCAL E PRAZOS DE ENTREGA DOS PRODUTOS E SERVIÇOS

7.1. Os produtos e serviços objeto deste Termo será executado no prédio Sede da PRODEPA, localizado na Rodovia Augusto Montenegro, KM 10, Tenoné, na cidade de Belém (PA).

7.2. O prazo máximo para a entrega dos itens pela CONTRATADA será de até 90 (noventa) dias corridos, contados a partir da data de solicitação.

7.3. A PRODEPA tem até 30 (trinta) dias corridos para emitir o Termo de Aceite Definitivo após o recebimento dos produtos ou serviços.

7.4. A PRODEPA tem até 15 (quinze) dias corridos para emitir o ateste da Nota Fiscal a emissão do Termo de Aceite Definitivo

8. PRAZO DE VIGÊNCIA

8.1. O contrato terá vigência pelo período de 36 (trinta e seis) meses, podendo ser prorrogado até o limite de 60 (sessenta) meses, contados a partir de sua celebração, com base no artigo 71, da Lei nº 13.303/2016, mediante justificativa.

9. CRITÉRIO DE REAJUSTE

9.1. Os critérios de reajustes são aqueles previstos no Anexo III da minuta do contrato.

10. SUBCONTRATAÇÃO

10.1. Não será admitida a subcontratação do objeto licitado.

11. GARANTIA DOS PRODUTOS E SERVIÇOS

11.1. A garantia deverá ser 36 (trinta e seis) meses, contados a partir da emissão do Termo de Aceite Definitivo do item contratado.

11.2. A garantia compreende o suporte técnico e garantia de funcionamento de todos os componentes, subsistemas, equipamentos, produtos, subscrições, softwares, subscrições,

assinaturas ou soluções descritas neste Termo de Referência.

11.3. Incluem-se nas manutenções corretivas e preventivas as atualizações tecnológicas dos programas da solução ofertada, de acordo com os seguintes:

11.4. As atualizações deverão cobrir todos os programas (software e firmware) adquiridos e incluir o fornecimento de correções (patches) e novas versões/revisões/distribuições (releases) assim que o FABRICANTE as torne disponíveis;

11.5. Entende-se por atualização de programas qualquer correção, pequena modificação, aperfeiçoamento (update), ou desenvolvimento de nova versão (upgrade) efetuado pelo fabricante para os produtos em questão;

11.6. Caso algum programa, módulo ou componente de programa seja descontinuado, deverá ser fornecido, como atualização descrita acima, outro que venha a ser desenvolvido com configuração (componente e/ou módulos) que lhe confiram toda a funcionalidade da última atualização fornecida;

11.7. Qualquer atualização, seja na forma de modificação, aperfeiçoamento ou produto inteiramente novo, deverá manter a funcionalidade mínima exigida da solução ofertada, independente de nomenclatura ou divisão do produto em módulos, pacotes, versão básica, avançada e outros.

11.8. As atualizações e correções (patches) dos produtos adquiridos deverão ser fornecidas em mídia CD (Compact Disc) ou DVD (Digital Video Disc), quando desta forma forem solicitadas ou, em não sendo possível, através de download pela internet.

11.9. Os serviços de garantia e suporte técnico serão realizados em dias úteis e não úteis (sábados, domingos e feriados), obedecendo aos níveis mínimos de serviço para atendimento definidos neste Termo de Referência.

11.10. Para abertura de solicitações de suporte técnico, incidentes, requisições, informações, reporte de incidentes e esclarecimento de dúvidas quanto à utilização de equipamentos/produtos e soluções fornecidas, a Contratada deverá possuir Central de Atendimento capaz de receber solicitações através dos canais abaixo:

11.10.1. Central de Atendimento telefônico 0800;

11.10.2. Sítio de Internet (Portal Web);

11.10.3. Correio Eletrônico, que forneça protocolos para acompanhamento do chamado,

11.11. As solicitações de suporte técnico deverão gerar registro contendo, no mínimo, as seguintes informações:

11.11.1. Informações de acompanhamento dos registros das ocorrências de problemas;

11.11.2. Identificação do registro (número do chamado);

11.11.3. Data e hora da abertura do chamado (registro);

11.11.4. Descrição do problema;

11.11.5. Identificação do reclamante (nome e telefone);

11.11.6. Data e hora de conclusão do atendimento (fechamento do chamado);

11.11.7. Ações realizadas para a solução do problema;

11.11.8. Identificação do técnico responsável pelo atendimento.

11.11.9. A **CONTRATADA** obrigatoriamente deverá informar o número do chamado em cada solicitação aberta.

11.12. Atendimento remoto: 24 horas por dia, 7 dias por semana.

11.13. Horário de funcionamento da central de atendimento telefônico: 24 horas por dia, 7 dias por semana.

11.14. A garantia ofertada deverá permitir a abertura de chamados direto com os respectivos **FABRICANTES** da solução, respeitando a política de cada **FABRICANTE**, de modo a ofertar flexibilidade para que a **CONTRATANTE** escolha onde abrir o chamado.

12. ACORDO DE NÍVEL DE SERVIÇO

12.1. Em relação aos produtos de hardware, o tempo de resposta e resolução para atendimento estarão relacionados à criticidade do chamado/incidente, devendo ser classificadas, em conformidade com tabela a seguir:

SEVERIDADE	PRAZO DE ATENDIMENTO	DESCRIÇÃO
1 (Urgente)	15 minutos	Problemas que geram parada total ou parcial na operação do ambiente
2 (Alta)	1 hora	Problemas que não geram parada total na operação do ambiente
3 (Média)	4 horas	Defeitos desconhecidos de *hardware* ou que tenham necessidade de alteração de código fonte do produto, atualização de versão, desde que não gerem paradas na operação do ambiente
4 (Baixa)	24 horas	Dúvidas em geral sobre o produto, funcionalidade ou configuração

12.2. Em relação aos produtos de software, o tempo de resposta para atendimento estarão relacionados à criticidade do chamado/incidente, devendo ser classificadas, em conformidade com tabela a seguir:

SEVERIDADE	PRAZO DE ATENDIMENTO	DESCRIÇÃO
1 (Urgente)	15 minutos	Os serviços de produção ou missão crítica estão inoperantes ou indisponíveis, seja em todo ou em parte; qualquer situação que coloque a produção ou os dados da CONTRATANTE ou de seus clientes, em risco de perda ou corrupção; Não existe uma solução de contorno disponível de imediato.
2 (Alta)	1 hora	Funcionalidades principais estão impactadas, reduzidas ou restritas ou não funcionais; qualquer operação que esteja rodando em modo restrito, mas que poderá afetar a produtividade em longo prazo ou que tenha alto impacto; Não existe uma solução de contorno temporária imediata.
3 (Média)	4 horas	Perda de funcionalidade parcial e não crítica; somente algumas operações específicas estão impactadas, mas não

SEVERIDADE	PRAZO DE ATENDIMENTO	DESCRIÇÃO
		comprometem grandes riscos à produtividade; Existe a possibilidade de o usuário/cliente continuar utilizando o software com baixo ou médio impacto; Existe uma solução de contorno temporária, ou ainda; Dúvida relativa à operação ou configuração ou erros em ambiente de homologação.
4 (Baixa)	24 horas	Perguntas genéricas em relação a utilização do software e pequenas correções que não envolvem nenhuma perda de funcionalidade; Qualquer situação que envolva baixo ou nenhum impacto para a produção; Dúvida relativa à operação ou configuração, pedidos de documentação.

12.3. Em relação aos serviços técnicos especializado, o tempo de resposta para atendimento estarão relacionados à criticidade do chamado/incidente, devendo ser classificadas, em conformidade com tabela a seguir:

SEVERIDADE	PRAZO DE ATENDIMENTO	DESCRIÇÃO
1 (Urgente)	2 horas	Os serviços de produção ou missão crítica estão inoperantes ou indisponíveis, seja em todo ou em parte; qualquer situação que coloque a produção ou os dados da CONTRATANTE ou de seus clientes, em risco de perda ou corrupção; Não existe uma solução de contorno disponível de imediato.
2 (Alta)	4 horas	Funcionalidades principais estão impactadas, reduzidas ou restritas ou não funcionais; qualquer operação que esteja rodando em modo restrito, mas que poderá afetar a produtividade em longo prazo ou que tenha alto impacto; Não existe uma solução de contorno temporária imediata.
3 (Média)	8 horas	Perda de funcionalidade parcial e não crítica; somente algumas operações específicas estão impactadas, mas não comprometem grandes riscos à produtividade; Existe a possibilidade de o usuário/cliente continuar utilizando o software com baixo ou médio impacto; Existe uma solução de contorno temporária, ou ainda; Dúvida relativa à operação ou configuração ou erros em ambiente de homologação.
4 (Baixa)	48 horas	Perguntas genéricas em relação a utilização do software e pequenas correções que não envolvem nenhuma perda de funcionalidade; Qualquer situação que envolva baixo ou nenhum impacto para a produção;

		Dúvida relativa à operação ou configuração, pedidos de documentação.

12.4. Em relação aos prazos estipulados, deverão ser considerados as seguintes premissas:

12.4.1. Por hora corrida entende-se aquela compreendida entre o período das 0h às 24h, 7 dias por semana, 365 dias por ano.

12.4.2. Por hora útil entende-se aquela compreendida entre o período das 08h às 18h, de segunda a sexta-feira, desde que dias úteis.

12.4.3. O prazo máximo para início de atendimento é contado a partir da abertura do chamado. É considerado início do atendimento a primeira resposta do time de suporte técnico da CONTRATADA que tratará do atendimento do chamado.

12.4.4. O prazo máximo para solução é contado a partir do término do prazo de início de atendimento.

12.4.5. Será admitida solução de contorno na resolução de chamados de severidade 1 e 2 para fins de atendimento dos prazos estipulados.

12.4.5.1. Entende-se por solução de contorno a redução ou eliminação do impacto de um incidente ou problema para o qual uma resolução completa ainda não está disponível ou não pode ser aplicada.

12.5. A CONTRATADA não será responsabilizada pelo não cumprimento de prazos de atendimento de chamados quando o chamado for originado por:

12.5.1. Falha, interrupção ou qualquer outra ocorrência nos serviços de telecomunicações ou energia elétrica que atendem à infraestrutura interna da CONTRATANTE;

12.5.2. Indisponibilidade de dados, inconsistência de dados e informações geradas pela CONTRATANTE;

12.5.3. Falha na infraestrutura de datacenter, infraestrutura de rede, hardware dos servidores e controladora de armazenamento (storage) e capacidade de ambiente de tecnologia da CONTRATANTE.

12.5.4. Bugs (problemas relacionados a código dos softwares) e/ou problemas conhecidos do software a serem sanados pelo próprio FABRICANTE.

12.5.5. Quaisquer intervenções no ambiente da SOLUÇÃO ou ambiente externo a esta que dependa exclusivamente da CONTRATANTE, na qual a CONTRATADA esteja impossibilitada de atuar, seja por acesso não permitido ou indisponibilidade de pessoal por parte da CONTRATANTE;

12.6. Qualquer descumprimento do acordo de nível de serviço será passível de punição, conforme as multas e penalidades descritas neste Termo de Referência no que tange ao acordo de nível de serviço.

13. GARANTIA DE EXECUÇÃO DO CONTRATO

13.1. A garantia de execução do contrato são aqueles previstos no Anexo III da minuta do contrato.

14. DA RESCISÃO

14.1. As condições de rescisão ou extinção desta contratação estão previstas no Anexo III da

minuta do contrato.

15. FISCALIZAÇÃO, CONTROLE E ACEITE DOS SERVIÇOS

15.1. A fiscalização, controle e aceite dos serviços objeto desta contratação estão previstos no Anexo III da minuta do contrato.

16. PAGAMENTO

16.1. A forma de pagamento é a prevista no Anexo III da minuta do contrato.

17. OBRIGAÇÕES DO CONTRATANTE DA CONTRATADA

17.1. As obrigações do contratante são aquelas previstas no Anexo III da minuta do contrato.

18. SANÇÕES ADMINISTRATIVAS.

18.1. As infrações e sanções são aquelas previstas no Anexo III da minuta do contrato.

19. PREVISÃO ORÇAMENTÁRIA

19.1. A contratação disposta neste Termo de Referência está de acordo com o Planejamento Plurianual (PPA), considerando o PROGRAMA – CIÊNCIA, TECNOLOGIA E INOVAÇÃO / AÇÃO – AMPLIAÇÃO E MODERNIZAÇÃO DA REDE DE TELECOMUNICAÇÃO.

20. DISPOSIÇÕES GERAIS

20.1. Com intuito de garantir a coesão e integração na execução/fornecimento, não será aceita a criação de consórcio para atender os requisitos definidos. Apenas a própria CONTRATADA deverá realizar a execução do objeto;

20.2. A LICITANTE deverá manter sigilo em relação aos dados, informações ou documentos que tomar conhecimento em decorrência da prestação dos serviços objeto desta contratação, bem como se submeter às orientações e normas internas de segurança da informação vigentes, devendo orientar seus empregados e/ou prepostos nesse sentido sob pena de responsabilidade civil, penal e administrativa.

ANEXO I-A
ESPECIFICAÇÕES TÉCNICAS

1. FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

1.1. CARACTERÍSTICAS GERAIS PARA FIREWALLS DE PRÓXIMA GERAÇÃO:

1.1.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.
1.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
1.1.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
1.1.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
1.1.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;
1.1.6. Todos os transceivers, cabos ou acessórios de conectividade com a rede deverão ser compatíveis e do mesmo fabricante dos equipamentos;
1.1.7. Todos os números referentes à capacidade/desempenho do(s) equipamento(s) devem ser comprovados utilizando-se da última versão estável dos softwares/componentes, não serão aceitos resultados com versões desatualizadas ou descontinuadas para comprovação.

1.2. FUNCIONALIDADES DE REDE E FIREWALL

1.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
1.2.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
1.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM);
1.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
1.2.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
1.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64 e PAT;
1.2.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
1.2.8. Deverá suportar sFlow ou Netflow;
1.2.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
1.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
1.2.11. Deve suportar o protocolo padrão da indústria VXLAN;
1.2.12. Deve implementar o protocolo ECMP;
1.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN e

situação do cluster;

1.2.14. Enviar log para sistemas de monitoração externos;

1.2.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

1.2.16. Deve possui mecanismos de proteção anti-spoofing;

1.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

1.2.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

1.2.19. Suportar OSPF graceful restart;

1.2.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

1.2.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

1.2.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

1.2.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

1.2.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;

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

1.2.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;

1.2.27. A solução deve suportar integração nativa com protocolo ACME, para obtenção de certificados válidos, de forma automática, como por exemplo Let's Encrypt ou ZeroSSL;

1.2.27.1. Caso a integração não seja nativa, será aceito formas de automação com o produto, isto é, que não haja interação humana por parte da CONTRATANTE. Esta automação deverá estar explicitamente detalhada na proposta referente ao serviço de implantação, bem como sendo realizada a sustentação da mesma no serviço de operação mensal.

1.2.28. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

1.2.29. Deverá suportar controle por zonas de segurança;

1.2.30. Deverá suportar controles de políticas por porta e protocolo;

1.2.31. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

1.2.32. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

1.2.33. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

1.2.34. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

1.2.35. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

1.2.36. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

1.2.37. Suporte a objetos e regras IPV6;

1.2.38. Suporte a objetos e regras multicast;

1.2.39. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.3. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

1.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

1.3.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
1.3.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
1.3.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
1.3.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
1.3.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
1.3.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
1.3.8. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
1.3.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;
1.3.10. Identificar o uso de táticas evasivas via comunicações criptografadas;
1.3.11. Atualizar a base de assinaturas de aplicações automaticamente;
1.3.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
1.3.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
1.3.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
1.3.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
1.3.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
1.3.17. Deve alertar o usuário quando uma aplicação for bloqueada;
1.3.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
1.3.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
1.3.20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;
1.3.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
1.3.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server,

Browse Based, Network Protocol, etc);

1.3.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

1.3.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

1.3.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

1.4. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

1.4.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

1.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

1.4.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

1.4.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

1.4.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

1.4.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

1.4.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

1.4.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.4.9. Deve permitir o bloqueio de vulnerabilidades;

1.4.10. Deve permitir o bloqueio de exploits conhecidos;

1.4.11. Deve incluir proteção contra-ataques de negação de serviços;

1.4.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

1.4.13. Detectar e bloquear a origem de portscans;

1.4.14. Bloquear ataques efetuados por worms conhecidos;

1.4.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

1.4.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.4.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

1.4.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

1.4.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

1.4.20. Identificar e bloquear comunicação com botnets;

1.4.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

1.4.22. Os eventos devem identificar o país de onde partiu a ameaça;

1.4.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião

(spyware) e worms;

1.4.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

1.4.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

1.4.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante;

1.4.27. Deve ser capaz de analisar em tempo real através de mecanismos baseados em Machine Learning o tráfego de ameaças avançadas de C2 (comando e controle) e spyware para proteção de ameaças de dia zero.

1.4.28. Deve ser capaz de aplicar de forma complementar às assinaturas de antivirus, a inspeção inline através de Machine learning em tempo real, bem como, prevenir ataques através do bloqueio efetivo do malware desconhecido (Dia Zero) capaz de analisar completamente o arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

1.4.29. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

1.4.30. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

1.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

1.5.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.5.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

1.5.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

1.5.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

1.5.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

1.5.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

1.5.7. Possuir pelo menos 70 (setenta) categorias de URLs;

1.5.8. Deve possuir a função de exclusão de URLs do bloqueio;

1.5.9. Permitir a customização de página de bloqueio;

1.5.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

1.5.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

1.5.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle

(C&C) de botnets conhecidas;

1.5.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

1.5.14. A funcionalidade de filtro de DNS deve proteger, em tempo real, contra ameaças de Tunelamento de DNS (DNS tunneling), infiltração de DNS (DNS infiltration), Servidores C&C e Algoritmos de Geração de Domínio (DGA).

1.6. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

1.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;

1.6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

1.6.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

1.6.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

1.6.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

1.6.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

1.6.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

1.6.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

1.6.9. Deve suportar autenticação de credenciais via RADIUS;

1.6.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

1.7. FUNCIONALIDADE DE DLP

1.7.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações, de pelo menos os seguintes protocolos: HTTP, FTP e SMTP;

1.7.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.7.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.7.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

1.7.5. Deve funcionar de maneira que consiga impedir que dados sensíveis saiam da rede e também deve funcionar de modo que se previna que dados não requisitados entrem na sua rede;

1.7.6. Deve possuir uma base de dados de dicionários e de padrões de dados pré-definidos,

tais como números de cartões de crédito, trechos de código fonte de software, etc. Essa base deve ser atualizada de forma automática pelo FABRICANTE da solução.

1.7.7. Deve permitir especificar a informação sensível a ser detectada como palavras, frases e expressões regulares.

1.7.8. Deve permitir a criação e armazenamento de impressões digitais (fingerprint) de documentos.

1.7.9. Deve inspecionar o conteúdo cookies HTTP em busca de informações sensíveis;

1.7.10. Deve permitir a aplicação de regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário autenticado;

1.7.11. Em tráfegos em que as regras definidas coincidirem, deve implementar no mínimo as seguintes ações: bloqueio, banimento e quarentena;

1.7.12. Deve armazenar, localmente ou na solução de gerenciamento centralizados de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP, em pelo menos os seguintes protocolos: E-mail, HTTP e mensageiros instantâneos;

1.7.13. Deve permitir a composição de uma ou mais regras DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego filtrado pelo sistema.

1.8. FUNCIONALIDADE DE GEOLOCALIZAÇÃO

1.8.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

1.8.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.9. FUNCIONALIDADE DE VPN

1.9.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.9.2. Suportar IPSec VPN;

1.9.3. Suportar SSL VPN;

1.9.4. A VPN IPSEc deve suportar 3DES;

1.9.5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

1.9.6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

1.9.7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

1.9.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

1.9.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI

1.9.10. Deve possuir interoperabilidade com, pelo menos, os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall, Sophos;

1.9.11. Suportar VPN IPSec em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

1.9.12. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

1.9.13. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

1.9.14. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

1.9.15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

1.9.16. Atribuição de DNS nos clientes remotos de VPN;

1.9.17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

1.9.18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

1.9.19. Suportar leitura e verificação de CRL (Certificate Revocation List);

1.9.20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que

circulam dentro dos túneis SSL;

1.9.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;

1.9.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;

1.9.23. Deverá manter uma conexão segura com o portal durante a sessão;

1.9.24. A funcionalidade de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 10 (32 e 64 bit) ou superior, Mac OS X (v11 ou superior), Linux (Ubuntu 18.04 ou superior, CentOS 7.4 ou superior, Red Hat 7.4 ou superior, iOS (versão 14 ou superior) e Android (versão 11 ou superior);

1.10. FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

1.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

1.10.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

1.10.2.1. Endereço de origem;

1.10.2.2. Endereço de destino;

1.10.2.3. Usuário e grupo;

1.10.2.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

1.10.2.5. Por porta;

1.10.3. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

1.10.4. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;

1.10.5. O QoS deve possibilitar a definição de fila de prioridade;

1.10.6. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

1.10.7. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

1.10.8. Suportar modificação de valores DSCP para o Diffserv;

1.10.9. Suportar priorização de tráfego usando informação de ToS (Type of Service);

1.10.10. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

1.10.11. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;

1.10.12. Deve possibilitar a definição de bandas distintas para download e upload;

1.11. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

1.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

1.11.2. A solução deve ser capaz de agregar vários links em uma interface virtual;

1.11.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (Por exemplo: O365 Exchange, AWS, Dropbox e etc);

1.11.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em

critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;

1.11.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;

1.11.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como por exemplo: Ping, HTTP, TCP ECHO, UDP ECHO, DNS e TCP Connect.

1.11.6.1. Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);

1.11.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).

1.11.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

1.11.8.1. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

1.11.8.2. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

1.11.8.3. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;

1.11.8.4. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;

1.11.9. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

1.11.10. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico OSPF e BGP;

1.11.11. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);

1.11.12. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

1.11.13. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

1.11.14. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

1.11.15. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de

pacotes que pode ocorrer durante o trânsito;

1.11.16. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

1.11.17. A solução deve suportar nativamente conectores com as principais clouds públicas (Exemplo: AWS, Oracle, Microsoft, Google);

1.11.18. Deve possibilitar a definição de largura de banda distintas nas interfaces/túneis para download e upload;

1.11.19. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

1.11.20. Deve implementar balanceamento de links;

1.11.21. Deve permitir definir a estratégia de balanceamento entre os links;

1.11.22. Deve suportar o balanceamento de, no mínimo, três links;

1.11.23. Deve suportar que um dos links seja definido como standby, no caso de acesso à Internet, onde apenas seja acionado na eventualidade de falha no link principal;

1.11.24. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

1.12. CARACTERÍSTICAS FÍSICAS DO EQUIPAMENTO/HARDWARE

1.12.1. Deverá ser homologado pela ANATEL, no que tange à equipamentos de telecomunicações, para comercialização em território nacional, conforme Resolução nº 715/2019, com certificado constando no Sistema de Certificação e Homologação acessível pelo sitio https://sistemas.anatel.gov.br/sch/ ou outro que o substituía;

1.12.2. Deve possuir fonte de alimentação AC Bivolt (mínimo de: 100-240 VCA e 50-60 Hz);

1.12.3. Deve possuir fonte redundante e Hot Swap para os equipamentos de firewall TIPO 01 e 02;

1.12.4. Deverá possuir o fluxo de ar da frente para trás (Front to Back) para os equipamentos de firewall TIPO 01 e 02;

1.12.5. Deverá possuir gabinete compatível com rack padrão 19";

1.12.5.1. Os equipamentos que possuem gabinete em formato diferente do especificado, deverão acompanhar o kit de conversão para que possam ser instalados/montados em rack padrão 19";

1.12.5.2. Somente serão aceitos acessórios originais do próprio FABRICANTE, não sendo permitidas nenhuma adaptação.

1.12.6. Deverá suportar temperatura operacional de, no mínimo, 5º C a 40º C;

1.12.7. Deverá suportar uma tolerância na umidade, no mínimo, 10% a 90%;

1.12.8. Deverá possuir conformidade (compliance), no mínimo, com: CB, FCC, CE e VCCI;

1.13. ITEM 01 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) – TIPO 01

1.13.1. Deve possuir garantia, suporte técnico, suporte a atualizações, serviço de RMA com entrega de equipamentos e peças em até 1 dia útil (NBD – Next Business Day) após diagnóstico e estar licenciado pelo período especificado com todas as funcionalidades que estão descritas nas especificações técnicas;

1.13.2. Deve suportar, no mínimo, 7 (sete) milhões de conexões simultâneas;

1.13.3. Deve suportar, no mínimo, 380 (trezentos e oitenta) mil de novas conexões por segundo;
1.13.4. Deve suportar, no mínimo, 40 (quarenta) Gbps de throughput VPN IPSec;
1.13.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 5.000 (cinco mil) túneis de VPN IPSEC Site-to-Site simultâneos;
1.13.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 30.000 (trinta mil) túneis de clientes VPN IPSEC simultâneos;
1.13.7. Deve suportar, no mínimo, 5.000 (cinco mil) clientes de VPN SSL simultâneos;
1.13.8. Deve suportar, no mínimo, 79 (sessenta e nove) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação e logging;
1.13.9. Deve suportar, no mínimo, 32 (trinta e dois) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware;
1.13.10. Deve possuir, pelo menos, 4 (quatro) interfaces 1/10 Gigabit Ethernet com conectores RJ-45;
1.13.11. Deve possuir, pelo menos, 8 (oito) interfaces 10 Gigabit Ethernet com conectores SFP+;
1.13.11.1. Será aceito também conectores SFP28 desde estes tenham suporte a conectores SFP+;
1.13.12. Deve possuir, pelo menos, 4 (quatro) interfaces 25 Gigabit Ethernet com conectores SFP28;
1.13.13. Deve possuir, pelo menos, 04 (quatro) interfaces 100 Gigabit Ethernet com conectores QSFP28 e suporte a conectores QSFP+ de 40 Gigabit Ethernet;
1.13.14. Deve possuir 1 (uma) Interface Gigabit Ethernet RJ45 dedicada para gerenciamento;
1.13.15. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;
1.13.16. Deverá acompanhar todos os cabos e transceivers necessários para a utilização em cluster de alta disponibilidade em plena capacidade.
1.13.17. Adicionalmente deverá ser entregue com os seguintes transceivers: 4x QSFP28 100GBase-SR4 e 4x SFP+ 10GBase-SR.

1.14. ITEM 02 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) – TIPO 02

1.14.1. Deve possuir garantia, suporte técnico, suporte a atualizações, serviço de RMA com entrega de equipamentos e peças em até 1 dia útil (NBD – Next Business Day) após diagnóstico e estar licenciado pelo período especificado com todas as funcionalidades que estão descritas nas especificações técnicas;
1.14.2. Deve suportar, no mínimo, 80 (oitenta) milhões de conexões simultâneas;
1.14.3. Deve suportar, no mínimo, 930 (novecentos e trinta) mil de novas conexões por segundo;
1.14.4. Deve suportar, no mínimo, 68 (sessenta e oito) Gbps de throughput VPN IPSec;
1.14.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 8.000 (oito mil) túneis de VPN IPSEC Site-to-Site simultâneos;
1.14.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 60.000 (sessenta mil) túneis de clientes VPN IPSEC simultâneos;
1.14.7. Deve suportar, no mínimo, 25.000 (vinte e cinco mil) clientes de VPN SSL simultâneos;

1.14.8. Deve suportar, no mínimo, 190 (cento e noventa) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação e logging;

1.14.9. Deve possuir, pelo menos, 16 (dezesseis) interfaces 10 Gigabit Ethernet com conectores SFP+;

1.14.9.1. Será aceito também conectores SFP28 desde estes tenham suporte a conectores SFP+;

1.14.10. Deve possuir, pelo menos, 4 (quatro) interfaces 100 Gigabit Ethernet com conectores QSFP28 e suporte a conectores QSFP+ de 40 Gigabit Ethernet;

1.14.11. Deve possuir 1 (uma) Interface Gigabit Ethernet RJ45 dedicada para gerenciamento;

1.14.12. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

1.14.13. Deverá acompanhar todos os cabos e transceivers necessários para a utilização em cluster de alta disponibilidade em plena capacidade.

1.14.14. Adicionalmente deverá ser entregue com os seguintes transceivers: 4x QSFP28 100GBase-SR4 e 8x SFP+ 10GBase-SR.

1.15. ITEM 03 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03

1.15.1. Deve possuir garantia, suporte técnico, suporte a atualizações, serviço de RMA com envio de equipamentos e peças em até 1 dia útil (NBD – Next Business Day) após diagnóstico e estar licenciado pelo período especificado com todas as funcionalidades que estão descritas nas especificações técnicas;

1.15.2. Deve suportar, no mínimo, 64 (sessenta e quatro) mil conexões simultâneas;

1.15.3. Deve suportar, no mínimo, 11 (onze) mil novas conexões por segundo;

1.15.4. Deve Suportar, no mínimo, 650 (seiscentos) Mbps de throughput VPN IPSec;

1.15.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;

1.15.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 250 (duzentos e cinquenta) túneis de clientes VPN IPSEC simultâneos;

1.15.7. Deve suportar, no mínimo, 20 (vinte) clientes de VPN SSL simultâneos;

1.15.8. Deve suportar, no mínimo, 1,5 (um virgula cinco) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação e logging;

1.15.9. Deve suportar, no mínimo, 800 (oitocentos) Mbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware;

1.15.10. Deve possuir, pelo menos, 1 (uma) interface com suporte a conectores SFP de 1 Gigabit Ethernet;

1.15.11. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet com conectores RJ-45;

2. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO, LOGS E RELATORIA

2.1. CARACTERÍSTICAS GERAIS

2.1.1. A arquitetura da solução deverá suportar que seja utilizado virtual appliance para o gerenciamento dos dispositivos de modo centralizado e um appliance físico para o

armazenamento e processamento de logs e relatoria com discos dedicados para esta tarefa sem depender da infraestrutura de armazenamento da CONTRATANTE.

2.1.2. Deve possuir garantia, suporte técnico, suporte a atualizações e estar licenciado com todas as funcionalidades descritas neste Termo de Referência pelo período especificado.

2.2. CARACTERÍSTICAS SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO – TIPO GERENCIA

2.2.1. Deve ser compatível para gerenciar os equipamentos de Firewalls de Próxima Geração (NGFW) considerando os modelos ofertados atendendo aos requisitos deste Item;

2.2.2. A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

2.2.3. Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2016 e KVM no RedHat 7 ou superiores;

2.2.4. Caso a solução seja entregue em appliance virtual, não deve possuir limite na licença ofertada para quantidade de vCPU e memória RAM;

2.2.5. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de vigência do contrato;

2.2.6. Possibilitar a criação e administração de políticas de Firewall, Controle de Aplicação, Sistema de Prevenção a Intrusão (IPS - Intrusion Prevention System), Antivírus, Filtro de Conteúdo e URL e Balanceamento inteligente de Links (SD-WAN);

2.2.7. Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;

2.2.8. Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados;

2.2.9. Permitir criar templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

2.2.10. Deve suportar o conceito de segregação de privilégios permitindo criar uma segregação no acesso administrativo de modo que uma determinada credencial ou grupo de credenciais de acesso só tenha acesso e visibilidade sobre os dispositivos escolhidos para aquela visão.

2.2.11. A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;

2.2.12. Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;

2.2.13. Permitir acesso concorrente de administradores e que seja definida uma cadeia de aprovação das alterações realizadas;

2.2.14. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

2.2.15. Permitir usar palavras chaves ou cores para facilitar identificação de regras;

2.2.16. Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;

2.2.17. Permitir criação de regras que fiquem ativas em horário definido;
2.2.18. Permitir criação de regras com data de expiração;
2.2.19. Realizar o backup das configurações para permitir o retorno de uma configuração salva;
2.2.20. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.
2.2.21. Gerar alertas automáticos via Email, SNMP e Syslog;
2.2.22. Deve ser permitido ao administrador transferir os backups para um servidor FTP, SCP ou SFTP.
2.2.23. Permitir backup das configurações e rollback de configuração para a última configuração salva;
2.2.24. Deve possibilitar a visualização e comparação de configurações atuais e configurações anteriores;
2.2.25. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
2.2.26. Deve suportar a distribuição e instalação remota de novas versões de software dos equipamentos, de forma remota e centralizada;
2.2.27. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;
2.2.28. Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.
2.2.29. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.
2.2.30. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.

2.3. ITEM 04 - GERENCIAMENTO DE LOGS E RELATORIA CENTRALIZADO – TIPO GERENCIA

2.3.1. A solução deverá ser ofertada em appliance virtual, sendo responsabilidade da CONTRATANTE a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;
2.3.2. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;
2.3.3. A solução deverá suportar o gerenciamento de dispositivos de, pelo menos, 100 (cem) dispositivos;
2.3.4. A solução deve permitir o empilhamento de licenças, ou seja, a compra de várias licenças, a fim de expandir o número de dispositivos suportados até um limite máximo de 1 (hum) mil dispositivos ou superior;
2.3.5. A solução deve ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2016/2019 e KVM no RedHat 7.1
2.3.6. A solução não deve possuir limite na quantidade de múltiplas vCPU;
2.3.7. A solução não deve possuir limite para suporte a expansão de memória RAM;

2.4. CARACTERÍSTICAS SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA – TIPO LOGS

2.4.1. Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;

2.4.2. Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;
2.4.3. Possuir suporte para SNMP versão 2 e 3;
2.4.4. Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;
2.4.5. Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;
2.4.6. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;
2.4.7. Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;
2.4.8. Deve suportar configurações de alta disponibilidade;
2.4.9. Deve permitir gerar alertas de eventos a partir de logs recebidos;
2.4.10. A solução deve ter relatórios predefinidos;
2.4.11. Permitir importação e exportação de relatórios
2.4.12. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
2.4.13. Suporte à geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
2.4.14. Suporte à geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
2.4.15. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
2.4.16. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
2.4.17. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
2.4.18. Deve ter a capacidade de criar relatórios no formato CSV, XML e PDF;
2.4.19. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;
2.4.20. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
2.4.21. Deve possuir mecanismos de remoção automática para logs antigos;
2.4.22. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
2.4.23. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
2.4.24. Permitir o envio por e-mail relatórios automaticamente;
2.4.25. Deve permitir que o relatório seja enviado por Email para o destinatário específico;
2.4.26. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
2.4.27. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
2.4.28. Deve permitir o uso de filtros nos relatórios;
2.4.29. Deve permitir a customização do design dos relatórios, pelo menos, permitindo a inserção de logo customizado do CONTRATANTE;
2.4.30. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
2.4.31. Deve permitir o envio automático de relatórios;
2.4.32. Deve permitir o envio automático dos logs para um servidor FTP, SFTP ou SCP;

2.4.32.1. Será também aceito que o gerenciador de log centralizado orquestre este envio automático através de políticas em cada equipamento gerenciado.

2.4.33. Deve permitir o envio automático de logs para armazenamento em nuvem para, pelo menos, as seguintes nuvens públicas: Amazon AWS, Microsoft Azure, Google Cloud Platform;

2.4.34. Deve permitir exportar os logs no formato CSV;

2.4.35. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

2.4.36. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

2.4.37. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

2.4.38. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

2.4.39. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

2.4.40. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

2.4.41. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

2.4.42. Deve permitir visualizar em tempo real os logs recebidos;

2.4.43. Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);

2.4.44. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

2.4.45. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

2.4.46. Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;

2.4.47. Deve possuir um painel de operações que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;

2.4.48. Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;

2.4.49. Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;

2.4.50. Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória)

2.4.51. Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;

2.4.52. Deve possuir relatório de uso de aplicações e mídias sociais;

2.4.53. Deve possuir relatório de prevenção de perda de dados (DLP);

2.4.54. Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;

2.4.55. Deve possuir relatório diário resumido de eventos e incidentes de segurança;

2.4.56. Deve possuir um relatório de tráfego DNS e e-mail;

2.4.57. Deve possuir relatório das 10 principais aplicações utilizadas na rede;

2.4.58. Deve possuir relatório dos 10 principais sites web utilizados na rede;

2.4.59. Deve possibilitar a visibilidade da utilização do balanceamento inteligente de links (SD-WAN), mostrando informações de utilização das regras por aplicação, largura de banda e níveis de serviços dos links (latência, Jitter e descarte de pacotes);

2.4.60. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;

2.4.61. Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;

2.4.62. Deve permitir a customização/criação de painel diversos, possibilitando a visualização em um dashboard de múltiplos painéis com as informações de recursos de rede e segurança;

2.4.63. Em caso de defeitos em peças/dispositivos que possuam armazenamento de dados, o serviço de RMA deve permitir a retenção, pelo cliente, dessas peças/dispositivos defeituosos, a fim de garantir o sigilo dos dados pessoais e dos dados críticos para o governo ali armazenados;

2.5. ITEM 05 - GERENCIAMENTO DE LOGS E RELATORIA CENTRALIZADO – TIPO LOGS

2.5.1. A solução deverá ser ofertada em appliance físico em hardware do próprio fabricante;

2.5.2. Deve possuir garantia, suporte técnico, suporte a atualizações, serviço de RMA com entrega de equipamentos e peças em até 1 dia útil (NBD – Next Business Day) após diagnóstico e estar licenciado pelo período especificado com todas as funcionalidades que estão descritas nas especificações técnicas;

2.5.3. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

2.5.4. A solução deve possuir a capacidade de coletar no mínimo 40.000 (quarenta mil) logs por segundo;

2.5.5. A solução deverá suportar o recebimento de logs de, pelo menos, 2.000 (dois mil) dispositivos;

2.5.6. A solução deverá possuir, no mínimo, 48 (quarenta e oito) TB de armazenamento liquido utilizável após RAID que possua tolerância à falha ou redundância de dados;

2.5.7. Deve possuir, pelo menos, 1 (uma) interface 1 Gigabit Ethernet com conectores RJ-45 para gerencia e configuração;

2.5.8. Deve possuir, pelo menos, 2 (duas) interfaces 10 Gigabit Ethernet com conectores SFP+ ou superior;

2.5.8.1. As interfaces deverão ser entregues com os transceivers populados prontas para uso.

2.5.9. Deve possuir discos hot-swap para armazenamento de dados, incluindo alta disponibilidade e redundância dos dados por tecnologia RAID.

2.5.10. Deve possuir fonte de alimentação redundante, hot-swap.

2.5.11. No caso da inexistência de appliances físicos, será aceito appliance virtual combinado à utilização de servidor de primeira linha com capacidades equivalentes para realizar o armazenamento, seja de modo interno ou externo ao próprio equipamento.

2.5.11.1. Somente serão aceitos servidores novos, de primeiro uso, sem previsão de fim de vida útil, montados em fábrica com datasheet comprobatório das capacidades, garantia e serviço de RMA com prazo e tempo de entrega equivalentes.

3. ACESSÓRIOS DE CONECTIVIDADE

3.1. ITEM 06 - TRANSCEIVER SFP+ 10GBase-SR

3.1.1. Transceiver SFP+ para conexão de fibras ópticas multimodo de até 400m em fibras OM4 e até 300m em fibras OM3;
3.1.2. Deve ser compatível com o padrão IEEE 802.3ae (10GBase-SR);
3.1.3. Deve ter velocidade de 10GbE;
3.1.4. Deve suportar a inserção a quente (Hot Plug);
3.1.5. Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

3.2. ITEM 07 - TRANSCEIVER SFP+ 10GBase-LR

3.2.1. Transceiver SFP+ para conexão de fibras ópticas monomodo de até 10Km;
3.2.2. Deve ser compatível com o padrão IEEE 802.3ae (10GBase-LR);
3.2.3. Deve ter velocidade de 10GbE;
3.2.4. Deve suportar a inserção a quente (Hot Plug);
3.2.5. Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

3.3. ITEM 08 - TRANSCEIVER SFP 1000Base-SX

3.3.1. Transceiver SFP para conexão de fibras ópticas multimodo de até 500m em fibras 50/125 µm e até 200m em fibras 62.5/125 µm;
3.3.2. Deve ser compatível com o padrão IEEE 802.3z (1000Base-SX);
3.3.3. Deve ter velocidade de 1GbE;
3.3.4. Deve suportar a inserção a quente (Hot Plug);
3.3.5. Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

3.4. ITEM 09 - TRANSCEIVER SFP 1000Base-LX

3.4.1. Transceiver SFP para conexão de fibras ópticas monomodo de até 10 Km;
3.4.2. Deve ser compatível com o padrão IEEE 802.3z (1000Base-LX);
3.4.3. Deve ter velocidade de 1GbE;
3.4.4. Deve suportar a inserção a quente (Hot Plug);
3.4.5. Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

3.5. ITEM 10 - TRANSCEIVER QSFP+ 40GBase-SR4

3.5.1. Transceiver QSFP+ para conexão de fibras ópticas multimodo de até 150m em fibras OM4 e até 100m em fibras OM3;
3.5.2. Deve ser compatível com o padrão IEEE 802.3ba (40GBase-SR4);
3.5.3. Deve ter velocidades de 40GbE;
3.5.4. Deve suportar a inserção a quente (Hot Plug);
3.5.5. Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

3.6. ITEM 11 - TRANSCEIVER QSFP28 100GBase-SR4

3.6.1. Transceiver QSFP28 para conexão de fibras ópticas multimodo de até 100m em fibras OM4;
3.6.2. Deve ser compatível com o padrão IEEE 802.3bm (100GBase-SR4);
3.6.3. Deve ter velocidades de 100GbE;
3.6.4. Deve suportar a inserção a quente (Hot Plug);
3.6.5. Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

4. ITEM 12 – SERVIÇO DE IMPLANTAÇÃO (INSTALAÇÃO, MIGRAÇÃO E ATUALIZAÇÃO) DA SOLUÇÃO – TIPO 01 E 02

4.1. Este serviço é compatível com os equipamentos firewalls TIPO 01 e 02;
4.2. Cada equipamento de firewall demandará 1 (uma) unidade do serviço de implantação,

isto é, se a solução adquirida vier a utilizar 2 (dois) equipamentos de firewall serão necessários 2 (duas) unidades deste serviço de implantação;

4.3. O Serviço de instalação, migração e atualização envolverá, no mínimo, as seguintes etapas:

4.3.1. Vistoria das instalações físicas e lógicas;

4.3.2. Descrição do plano de implantação;

4.3.3. Cronograma;

4.3.4. Topologia e Arquitetura;

4.3.5. Plano de Recuperação (rollback), caso a mudança não seja bem sucedida;

4.3.6. Rotinas mínimas para a manutenção dos equipamentos;

4.4. Após aceite do plano de implantação por parte do CONTRATANTE, a CONTRATADA deve instalar e configurar o produto, permitindo ao CONTRATANTE executar seus próprios testes antes de autorizar a janela de migração final do equipamento.

4.5. A CONTRATADA deve auxiliar a CONTRATANTE na atualização de políticas de firewall, logging, topologias e demais correlatos apresentando as melhores práticas de mercado, as práticas que melhor se adequem a realidade do CONTRATANTE e de uso dos equipamentos e software desta contratação.

4.6. No dia da migração, por ser considerado uma atividade critica, obrigatoriamente será necessária a presença física nas instalações da CONTRATANTE;

4.6.1. O local a ser considerado para esta atividade está localizado na cidade de Belém/PA, na Rod Augusto Montenegro, Km 10 – Centro Administrativo do Estado, Bairro Tenoné, CEP 66820-000

4.7. O serviço de instalação, migração e configuração deverá contemplar, no mínimo, as seguintes atividades:

4.7.1. Vistoria das instalações existente;

4.7.2. Avaliação do ambiente de rede físico e lógico existente;

4.7.3. Instalação física dos equipamentos;

4.7.4. Configurações iniciais dos equipamentos;

4.7.5. Backup da solução existente;

4.7.6. Descomissionamento da solução existente;

4.7.7. Instalação da nova solução adquirida;

4.7.8. Integração no gerenciamento centralizado;

4.7.9. Integração na coleta de log centralizada;

4.7.10. Migração das configurações existente para a nova solução, incluindo possíveis adaptações caso necessário;

4.7.11. Testes de funcionamento da solução;

4.7.12. Atualização das versões dos firmwares/softwares;

4.7.13. Acompanhamento pós migração para avaliação do funcionamento.

4.8. As atividades do item anterior não são exaustivas, uma vez que a CONTRATADA poderá identificar demais atividades que sejam pertinentes para o perfeito funcionamento do serviço garantindo o sucesso da operação. Tais atividades são de exclusiva responsabilidade da CONTRATADA não gerando nenhum custo adicional ao CONTRATANTE;

4.9. As atividades de migração que impactem em parada do ambiente deverão ser realizadas fora do horário do comercial, preferencialmente agendada para um final de semana ou feriado.

4.10. Ao final da execução do plano de implantação deve-se apresentar o documento final de implantação do tipo as-built. Somente após a aprovação deste documento o serviço será considerado como concluído.

4.11. Deverá contemplar serviço de conversão e migração de regras e configurações, a ser usado uma única vez no momento da implantação, e que suporte como origem, no mínimo, os

maiores fabricantes de firewall de próxima geração, conforme pesquisa do IDC (Checkpoint, Cisco, Fortinet, Palo Alto Networks e SonicWall).

4.11.1. Deverá obrigatoriamente ser compatível com o equipamento existente Palo Alto PA-5220, PAN-OS versão 10.2 ou superior;

4.12. As soluções implantadas devem ser validadas e homologadas pelo FABRICANTE das soluções, e ao final da implantação deve ser enviado a declaração do mesmo informando tal condição. Cabe a CONTRATADA acionar os serviços técnicos profissionais e avançados do FABRICANTE para atingir este objetivo;

4.13. Por fim, deverá incluir a transferência de conhecimento das atividades realizadas e da solução implantada para a equipe técnica local, com no mínimo, 3 (três) dias de duração;

4.13.1. Esclarece-se que o repasse de conhecimento é para tratar dos pontos que foram realizados na implantação, bem como operações básicas e rotineiras para o entendimento das atividades realizada e se trata de treinamento oficial.

5. ITEM 13 – SERVIÇO DE IMPLANTAÇÃO/INSTALAÇÃO DE FIREWALL – TIPO 03

5.1. Este serviço é compatível com os equipamentos firewalls TIPO 03;

5.2. Cada equipamento de firewall demandará 1 (uma) unidade do serviço de implantação, isto é, se a solução adquirida necessitar de instalação de 30 (trinta) equipamentos de firewall serão necessários 30 (trinta) unidades deste serviço de implantação;

5.3. O Serviço de instalação envolverá, no mínimo, as seguintes etapas:

5.3.1. Descrição de atividades;

5.3.2. Cronograma de instalação;

5.4. Após aceite do plano de implantação por parte do CONTRATANTE, a CONTRATADA deve instalar e configurar o produto, permitindo ao CONTRATANTE executar seus próprios testes, caso exigido.

5.5. A CONTRATADA deve auxiliar a CONTRATANTE na atualização de políticas de firewall, logging, topologias e demais correlatos apresentando as melhores práticas de mercado, as práticas que melhor se adequem a realidade do CONTRATANTE e de uso dos equipamentos e software desta contratação.

5.6. A instalação física do equipamento poderá ocorrer em qualquer local da Região Metropolitana de Belém;

5.7. O serviço de instalação, migração e configuração deverá contemplar, no mínimo, as seguintes atividades:

5.7.1. Avaliação do ambiente de rede existente;

5.7.2. Instalação física dos equipamentos;

5.7.3. Configurações iniciais dos equipamentos;

5.7.4. Integração no gerenciamento centralizado;

5.7.5. Integração na coleta de log centralizada;

5.7.6. Interligação com a rede/topologia existente de forma segura;

5.7.7. Migração/adaptação de configurações existente para a nova solução;

5.7.8. Criação de regras básicas de proteção/segurança;

5.7.9. Testes de funcionamento da solução;

5.7.10. Atualização das versões dos firmwares/softwares;

5.8. As atividades do item anterior não são exaustivas, uma vez que a CONTRATADA poderá identificar demais atividades que sejam pertinentes para o perfeito funcionamento do serviço garantindo o sucesso da operação. Tais atividades são de exclusiva responsabilidade da CONTRATADA não gerando nenhum custo adicional ao CONTRATANTE;

5.9. Ao final da execução do plano de implantação deve-se apresentar o documento final de

implantação do tipo as-built. Somente após a aprovação deste documento o serviço será considerado como concluído.

6. ITEM 14 - TREINAMENTO DA SOLUÇÃO

6.1. Treinamento oficial das soluções fornecidas. Considerando a diversidade dos treinamentos da solução de firewall, log centralizado e relatoria será aceito a composição de 2 (dois) ou mais cursos para compor a ementa do conteúdo;
6.2. Treinamento a ser realizado para até 8 (oito) participantes;
6.3. Deverá ser abordado conceitos teóricos e atividades práticas de laboratório;
6.4. Todos os treinamentos poderão ser realizados de forma remota/tele presencial;
6.5. O idioma das aulas deverá ser em português;
6.6. Deverá ser entregue material didático composto de apostila em formato digital ou impresso. O material didático poderá ser em português ou inglês.
6.7. Carga horária mínima de 72 (setenta e duas) horas;
6.8. Deverá ser abordado, no mínimo, os seguintes tópicos:
6.8.1. Configurações iniciais e avançadas;
6.8.2. Configurações de VLANs, LACP, DHCP e tipos de NAT;
6.8.3. Políticas de segurança;
6.8.4. Prevenção de ameaças, anti-malware, filtro URL e controle de aplicações;
6.8.5. Identificação de usuários, qualidade de serviço e regras por aplicação;
6.8.6. Filtro de dados;
6.8.7. VPN Site-to-Site e Client-To-Site;
6.8.8. SD-WAN e Overlay;
6.8.9. Roteamento estático e dinâmico;
6.8.10. ZTNA;
6.8.11. Análise de malwares modernos;
6.8.12. Alta disponibilidade;
6.8.13. Gerenciamento centralizado e relatórios;
6.8.14. Avaliação de boas práticas;
6.8.15. Monitoramento de capacidade dos equipamentos;
6.8.16. Diagnóstico e resolução de problemas;
6.8.17. Otimização de políticas de firewall.
6.8.18. Configuração, visualização e gerenciamento de logs;
6.8.19. Configuração, visualização e gerenciamento de relatórios;
6.8.20. Gerenciamento de eventos, incidentes e recursos de automação (playbooks);
6.8.21. Configuração e administração de instâncias de virtualização.
6.9. Ao final de cada treinamento deverá ser emitido certificado de conclusão a cada participante, devidamente assinado pela empresa promovente, especificando conteúdo programático completo do curso, corpo docente e carga horária.
6.10. Ao final de cada treinamento será realizado uma avaliação do mesmo pela própria CONTRATANTE com os alunos. Caso o treinamento seja considerado como insatisfatório ou insuficiente, este deverá ser realizado até que o mesmo seja considerado como satisfatório.

7. ITEM 15 - SERVIÇO TÉCNICO ESPECIALIZADO DE OPERAÇÃO ASSISTIDA E MONITORAMENTO

7.1. O serviço de Suporte Técnico Especializado, Monitoramento e Operação Assistida, doravante denominado apenas por suporte técnico, se iniciará após a implantação. As ferramentas necessárias à execução desses serviços serão de responsabilidade da CONTRATADA;

7.2. Qualquer requisito de infraestrutura, seja de hardware, software ou serviços, para implementação do acesso remoto ao ambiente computacional da CONTRATANTE, será de inteira responsabilidade da CONTRATADA, não devendo haver qualquer ônus ou custo adicional à CONTRATANTE;

7.3. A CONTRATADA deverá possuir central de atendimento própria para realizar os atendimentos de chamados no regime de 24x7, isto é, 24 horas por dia, 7 dias por semana, 365 dias por ano;

7.4. O suporte técnico também contempla, no mínimo, as seguintes atividades:

7.4.1. Consultoria sob demanda e operação assistida sob demanda;

7.4.2. Execução de atividades operacionais, utilizando os procedimentos mais adequados e adaptados à realidade do ambiente do CONTRATANTE;

7.4.3. Elaboração de procedimentos especiais ou detalhamento de procedimentos padrões, documentados e adaptados à realidade do ambiente do CONTRATANTE;

7.4.4. Elaboração de relatórios de atividades, detalhando os procedimentos realizados e eventuais ajustes, se necessário;

7.4.5. Garantia de que a solução seja operada seguindo procedimentos de melhores práticas;

7.4.6. Garantia, por meio de consultoria e operação assistida, de mais desempenho e disponibilidade da SOLUÇÃO;

7.4.7. Atuar na tratativa de incidentes, requisições de serviço, mudanças e problemas, observando os respectivos processos de gestão e os acordos de nível de serviço (ANS), para os itens de configuração cobertos pelo escopo contratado;

7.4.8. Elaborar análises de causa-raiz em resposta ao processo de gestão de problemas e/ou incidentes críticos;

7.4.9. Aplicar os patches de correção de vulnerabilidades disponibilizadas pelo fornecedor, de acordo com o calendário definido no tópico de segurança e resiliência, desde que não impliquem em upgrade de versão;

7.4.10. Abrir chamados técnicos em situações críticas, quando necessário, assim como fazer escalada de chamados e incidentes através do portal do FABRICANTE;

7.4.11. Configurar a solução de acordo com os requisitos específicos de segurança da CONTRATANTE;

7.4.12. Implementar regras de segurança, políticas de acesso e outras configurações necessárias;

7.4.13. Realizar testes abrangentes para verificar a segurança e a funcionalidade do firewall;

7.4.14. Testar a eficácia das políticas de segurança e regras de acesso;

7.4.15. Executar simulações de ataque para testar a robustez da solução;

7.4.16. Desenvolver e fornecer documentação sobre as configurações da solução, políticas implementadas, e procedimentos operacionais;

7.4.17. Monitorar constantemente capacidade e o desempenho da solução afim garantir que ele possa lidar com aumento do tráfego de rede e as demandas de segurança;

7.4.18. Estabelecer procedimentos de monitoramento contínuo para detectar e responder a ameaças de segurança;

7.4.19. Implementar atualizações regulares e patches de segurança para garantir que a solução esteja protegida contra ameaças emergentes;

7.4.20. Realizar auditorias de segurança periódicas para avaliar a eficácia da solução e fazer ajustes conforme necessário;

7.4.21. Garantir a integração adequada da solução com outros ecossistemas compatíveis e a infraestrutura local;

7.4.22. Preparar relatórios detalhados sobre a eficiência da solução, incluindo estatísticas e

tráfego, ameaças bloqueadas e quaisquer incidentes de segurança;

7.4.23. Avaliar em conjunto com a equipe de segurança interna da CONTRATANTE afim de identificar áreas de melhoria;

7.4.24. Planejar atualizações futuras ou expansões da solução, conforme necessário, para acompanhar o crescimento organizacional.

7.5. O rol de atividades especificado no item anterior não é uma lista exaustiva de todos as atividades, uma vez que considerando a grande complexidade do ambiente e uma extensa gama de atividades que são necessárias para o perfeito funcionamento da solução, a CONTRATANTE é inteiramente responsável pelo bom funcionamento dos equipamentos e da solução como um todo, de tal forma que caso seja necessário a execução de algum serviço que não esteja listado acima deverá ser realizado sem custos adicionais para garantir o pleno funcionamento da solução.

7.5.1. Estas atividades são estritamente relacionadas aos equipamentos que compõem a solução e não irão se estender para serviços, equipamentos ou atividades que não estejam especificados neste Termo de Referência.

7.6. Cumprir, assistência presencial, nos dias úteis, em horário comercial entre 08:00 e 18:00 horas em visitas agendadas (doravante denominadas como “Reunião Periódica”) com duração mínima de, pelo menos, 3 (três) dias;

7.7. Cumprir calendário de, Reunião Periódica, com a realização de visitas e reuniões periódicas a cada 03 (três) meses;

7.7.1. Ficará a cargo da CONTRATANTE decidir por acumular ou não, a reunião periódica, em razão da execução do contrato, sem prejuízo a CONTRATADA.

7.8. A cada trimestre deverá ser realizado um healthcheck em conjunto com o FABRICANTE no ambiente da CONTRATANTE para medir a saúde do mesmo.

7.9. Além disto a CONTRATADA se obriga a contratar diretamente com o FABRICANTE para ofertar os serviços de:

7.9.1. Trabalhos de Consultoria e Arquitetura: em que seja necessário a mudança do desenho da implantação original, ou resizing do ambiente da CONTRATANTE, ou análise para atualização de produtos, ou adição de novos itens a partir da detecção de vulnerabilidades excepcionais;

7.9.2. Trabalhos de Tunning: Em que se faça necessária a otimização de recursos, dos ajustes finos a partir da detecção de gargalos de performance;

7.9.3. Validação e/ou Homologação após alterações no ambiente: para validação, homologação, e/ou verificação de melhores práticas, de novas configurações ou recursos que venham a ser habilitados nas soluções implantadas após término da implantação inicial;

7.9.4. Avaliação Recorrente: para avaliações periódicas, em periodicidade a ser definida pela CONTRATANTE, visando a validação, homologação, e/ou verificação do uso de melhores práticas nas soluções implantadas;

7.9.5. Aplicações de configurações e resoluções de problemas avançados que saiam do contexto e do cotidiano da equipe técnica da CONTRATANTE;

7.9.6. Serviços Profissionais para integração de novos produtos, de fabricantes diversos, de hardware e software que venham a ser adquiridos e implantados na rede da CONTRATANTE;

7.10. Os serviços profissionais do FABRICANTE supracitados poderão ser utilizados a cada ano, com limite máximo de, pelo menos, 160 (cento e sessenta) horas.

7.11. Antes do consumo das horas técnicas, uma reunião de alinhamento deverá ser realizada entre o CONTRATANTE, a CONTRATADA e o FABRICANTE, para estabelecimento do escopo dos serviços e do total de horas técnicas que serão consumidos. Somente após o aceita da

CONTRATANTE os serviços poderão ser iniciados.

7.12. O consumo das horas técnicas de serviço será sob demanda, em pacotes de 8 horas úteis, correspondente a 1 dia de trabalho.

7.13. O serviço técnico especializado já inclui os serviços do FABRICANTE, devendo ser respeitado o limite máximo de horas, bem como deverá ser distribuído ao longo do período para garantir o pleno funcionamento da solução em conjunto com as melhores práticas do FABRICANTE.

7.14. O suporte técnico será prestado 24 horas por dia, 7 dias por semana, mediante requisição (abertura de chamado) da CONTRATANTE. Para tanto, a CONTRATADA deverá fornecer suporte telefônico (Central de Atendimento) para acionamento além de plataforma de abertura de chamados via WEB.

7.14.1. Para cada solicitação de atendimento técnico, deverá ser gerado um identificador único (protocolo) para fins de controle e acompanhamento. A CONTRATADA deverá informar esse identificador da CONTRATANTE, bem como manter o histórico de ações e atividades nos chamados realizados durante toda a vigência contratual.

7.14.2. Para cada chamado técnico, a CONTRATADA deverá respeitar os seguintes prazos máximos para atendimento conforme o nível de criticidade e prazos abaixo. O prazo será contado a partir da abertura do chamado;

7.14.3. A CONTRATADA deverá disponibilizar mensalmente a relação dos chamados contendo as seguintes informações:

7.14.3.1. Número do chamado;
7.14.3.2. Serviço (catálogo);
7.14.3.3. Defeito relatado;
7.14.3.4. Solução;
7.14.3.5. Status (Situação);
7.14.3.6. Data e hora de abertura do chamado;
7.14.3.7. Data e hora do encerramento do chamado (se encerrado);
7.14.3.8. Data e hora prevista de solução (não encerrado);
7.14.3.9. Houve reabertura do chamado (sim/não);
7.14.3.10. Severidade;
7.14.3.11. Solicitante;
7.14.3.12. Atendente;
7.14.3.13. Tempo decorrido (em minutos);

7.15. A disponibilização dos dados, que será definida a critério da CONTRATANTE, deverão ser feitos via e-mail ou disponibilização do acesso à base de dados da ferramenta de chamado da CONTRATADA.

7.16. A CONTRATADA deverá disponibilizar seu corpo técnico para atendimento presencial em incidentes ou solicitação de alta complexidade e criticidade, caso seja, por necessidade ou solicitação, de comum acordo entre CONTRATADA e CONTRATANTE.

7.17. A periodicidade de medição e aferição de desempenho dos chamados técnicos deverá ser realizado de forma mensal, obedecendo a seguinte fórmula abaixo:

Fórmula: ICAP = (QCAP / TCA) x 100
ICAP= Índice (%) de Chamados Atendidos no Prazo
QCAP= Quantidade de Chamados Atendidos no Prazo
TCA = Total de Chamados Atendidos

7.18. A equipe técnica da CONTRATADA deverá ser composta, por pelo menos, 01 (um) perfil

profissional qualificado, para garantir a execução do serviço com qualidade e segurança, devendo possuir certificação(ões) compatível(eis) com os produtos da solução ofertada.

7.19. Em relação a composição do perfil profissional e as exigências:

7.19.1. Caso tenha alteração no nome da certificação antes ou durante a execução do CONTRATO, será permitida apresentação da sua equivalência sem prejuízo a CONTRATADA;

7.19.2. Será aceito os casos em que os profissionais da CONTRATADA possuem certificações superiores ou em versões mais avançadas;

7.20. Os perfis profissionais devem ser obedecidos e atendidos no início da prestação dos serviços de suporte técnico e permanecer válidos durante toda a vigência do contrato;

7.20.1. Sempre que houver atualização dos profissionais a CONTRATADA deverá ser informada dos novos profissionais que compõem a equipe;

7.20.2. Não será permitido que a CONTRATADA fique por mais de 60 (sessenta) dias consecutivos sem os respectivos profissionais para prestação do serviço adequado.

Proposta Comercial

A EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO PARÁ - PRODEPA.

Nº Proposta: 28/05/2025

Versão Proposta: 01 Brasília, 28 de maio de 2025.

2. Nossos Parceiros

1. Apresentação da Empresa

1.1. Sobre nós

A Alltech Soluções em Tecnologia é uma empresa focada em soluções e serviços de TI, com mais de 08 anos de experiência no mercado nacional no setor público, com sede em Brasília/DF e atuação em 13 Estados brasileiros. Especializada em consultoria em TI, desenvolvimento de aplicações, automação, segurança da informação, cloud, gestão de TI, DevOps e suporte técnico, a Alltech conta com uma equipe de profissionais altamente capacitados e tecnologias de ponta para garantir a eficiência e a segurança dos serviços prestados. Temos como objetivo principal ajudar nossos clientes a alcançarem seus objetivos de negócio por meio da tecnologia, oferecendo soluções inovadoras e personalizadas para cada necessidade.

1.2. Certificação de Transparência CertiGov

A Alltech Soluções em Tecnologia, acaba de conquistar a certificação de transparência **CertiGov**, na classe bronze. O selo atesta as ações de integridade da empresa em seus processos, política e cultura ética. Com o certificado, a Alltech fomenta a segurança de sua cadeia de atuação para vendas ao governo, e se antecipa à demanda crescente por práticas de compliance aos fornecedores dos setores público e privado.

As empresas que conquistam o **CertiGov** demonstram seu posicionamento contra a corrupção e contra o suborno, demonstrando que tem os conceitos disseminados em sua organização e colaboradores, e implantam boas práticas para reduzir os riscos de envolvimento em ações ilícitas. O processo de certificação da Alltech Soluções em Tecnologia incluiu uma avaliação detalhada dos processos, riscos e aderência a rigorosos padrões de integridade e treinamentos.

2.Nossos Parceiros

3.Proposta Técnica/Comercial

3.1 Valor da Proposta

OBJETO: Registro de Preço para aquisição de solução firewall com treinamento e serviços técnicos especializados com instalação, configuração, operação assistida e continuada pelo período de 36 (trinta e seis) meses.

PROPOSTA COMERCIAL						
ITEM	DESCIÇÃO	MARCA/MODELO	UNIDADE	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Firewall de Próxima Geração (NGFW) – TIPO 01	FORTINET / FG-3000F	Und	2	R$ 3.230.524,97	R$ 6.461.049,94
2	Solução de Firewall de Próxima Geração (NGFW) – TIPO 02	FORTINET / FG-3700F	Und	2	R$ 7.889.467,62	R$ 15.778.935,25
3	Solução de Firewall de Próxima Geração (NGFW) – TIPO 03	FORTINET / FG-80F	Und	350	R$ 42.209,40	R$ 14.773.290,23
4	Gerenciamento Centralizado de Logs e Relatoria – TIPO GERENCIA	FORTINET/ FORTIMANAGER	Und	4	R$ 139.628,93	R$ 558.515,71
5	Gerenciamento Centralizado de Logs e Relatoria – TIPO LOGS	FORTINET / FORTIANALYZER	Und	3	R$ 2.438.581,87	R$ 7.315.745,60
6	Transceiver SFP+ 10GBase-SR	FORTINET / FN-TRAN-SFP+SR	Und	24	R$ 817,28	R$ 19.614,63
7	Transceiver SFP+ 10GBase-LR	FORTINET / FN-TRAN-SFP+LR_SC	Und	24	R$ 1.514,00	R$ 36.335,91
8	Transceiver SFP 1000Base-SX	FORTINET / FN-TRAN-SX	Und	300	R$ 500,03	R$ 150.008,05
9	Transceiver SFP 1000Base-LX	FORTINET / FN-TRAN-LX	Und	50	R$ 1.025,29	R$ 51.264,36
10	Transceiver QSFP+ 40GBase-SR4	FORTINET / FN-TRAN-QSFP+SR	Und	16	R$ 4.095,34	R$ 65.525,49
11	Transceiver QSFP28 100GBase-SR4	FORTINET/FN-TRAN-QSFP28-SR	Und	8	R$ 9.983,81	R$ 79.870,47
12	Serviço de Implantação (Instalação, Migração e Atualização) da Solução – TIPO 01 e 02	ALLTECH	Und	4	R$ 67.497,00	R$ 269.988,00
13	Serviço de Implantação/Instalação de Firewall – Tipo 03	ALLTECH	Und	350	R$ 5.512,89	R$ 1.929.511,50
14	Treinamento da Solução	OFICIAL FORTINET	Turma	4	R$ 816.335,47	R$ 3.265.341,88
15	Serviço técnico especializado para operação continua e monitoramento, incluindo suporte preventivo e corretivo para Solução de Firewall	ALLTECH	Mês	36	R$ 94.519,22	R$ 3.402.691,92
					Valor Global	**R$ 54.157.688,94**

Valor por extenso global: R$54.157.688,94 (Cinquenta e quatro milhões, cento e cinquenta e sete mil, seiscentos e oitenta e oito reais e noventa e quatro centavos).

3.Proposta Técnica/Comercial

Segue abaixo a planilha detalhada com os devidos Part Numbers de cada item:

ITEM	PARTNUMBER	DESCRIÇÃO
1	FG-3000F	FortiGate-3000F 6 x 100GE QSFP28 slots , 16 x 10GE SFP+/25GE SFP28 slots (including 14x ports, 2x HA ports), 18x 10G Base-T (including 2x MGMT ports), SPU NP7 and CP9 hardware accelerated, and 2 AC power supplies
	FC-10-F3K0F-809-02-36	FortiGate-3000F 3 Year Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium)
	FC-10-F3K0F-204-02-36	FortiGate-3000F 3 Year Upgrade FortiCare Premium to Elite (Require FortiCare Premium)
	FC-10-F3K0F-210-02-36	FortiGate-3000F 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite)
	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m 10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots.
	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots
	FN-TRAN-QSFP28-SR	100GE QSFP28 transceivers 100GE QSFP28 transceiver module, 4 channel parallel fiber, short range for systems with QSFP28 Slots
2	FG-3700F	FortiGate-3700F 4x 400 GE QSFP-DD slots, 4x ULL SFP28 slots and 20x 50 GE SFP56 slots (including 18x ports, 2x HA ports), 2x 10GE RJ45 Management Ports, SPU NP7 and CP9 hardware accelerated, and 2 AC power supplies
	FC-10-F3K7F-809-02-36	FortiGate-3700F 3 Year Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium)
	FC-10-F3K7F-204-02-36	FortiGate-3700F 3 Year Upgrade FortiCare Premium to Elite (Require FortiCare Premium)
	FC-10-F3K7F-210-02-36	FortiGate-3700F 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite)
	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m 10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots.
	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots
	FN-TRAN-QSFP28-SR	100GE QSFP28 transceivers 100GE QSFP28 transceiver module, 4 channel parallel fiber, short range for systems with QSFP28 Slots
3	FG-80F	FortiGate-80F 8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports.
	FC-10-0080F-809-02-36	FortiGate-80F 3 Year Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium)
	FC-10-0080F-204-02-36	FortiGate-80F 3 Year Upgrade FortiCare Premium to Elite (Require FortiCare Premium)
	SP-RACKTRAY-02	Rack mount tray Rack mount tray for all FortiGate E series and F series desktop models and backward compatible with SP-RackTray-01. For list of compatible FortiGate products, visit Documentation website.
4	FMG-VM-100-UG	FortiManager - VM License Upgrade license for adding 100 Fortinet devices/Virtual Domains; allows for total of 5 GB/Day of Logs.
	FC4-10-M3004-285-02-36	FortiManager-VM FortiCare Elite Support 3 Year FortiCare Elite Support (1 - 1010 devices/Virtual Domains)
5	FAZ-3100G	FortiAnalyzer-3100G
	FC-10-AZ31G-466-02-36	FortiAnalyzer-3100G Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Service)
	FC-10-AZ31G-204-02-36	FortiAnalyzer-3100G Upgrade FortiCare Premium to Elite (Require FortiCare Premium)
	FC-10-AZ31G-210-02-36	FortiAnalyzer-3100G Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite)
	FC-10-AZ31G-301-02-36	FortiAnalyzer-3100G Secure RMA Service
	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots
	FC-10-FAZ00-286-02-36	FAZ Backup to Cloud Service 1 Year Subscription to FortiAnalyzer storage connector service for 10TB data transfer to public cloud.
6	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots
7	FN-TRAN-SFP+LR	10GE SFP+ transceiver module, long range 10GE SFP+ transceiver module, 10km long range for systems with SFP+ and SFP/SFP+ slots
8	FN-TRAN-SX	1GE SFP SX transceiver module 1GE SFP SX transceiver module for systems with SFP and SFP/SFP+ slots
9	FN-TRAN-LX	1GE SFP LX transceiver module 1GE SFP LX transceiver module, 10km range, -40C to 85C, over SMF, for systems with SFP and SFP/SFP+ slots.
10	FN-TRAN-QSFP+SR	40GE QSFP+ transceivers, short range 40GE QSFP+ transceiver module, short range for systems with QSFP+ Slots
11	FN-TRAN-QSFP28-SR	100GE QSFP28 transceivers 100GE QSFP28 transceiver module, 4 channel parallel fiber, short range for systems with QSFP28 Slots

3.2. Condições de Pagamento

O pagamento será realizado no conforme ao item 8 PRAZOS, RECEBIMENTO E CONDIÇÕES DE PAGAMENTO – do Termo de Referência.

8.1 O pagamento será realizado em uma única parcela após a emissão do Termo de Aceite Definitivo do respectivo serviço ou produto.
8.1.1 Exceto para o serviço técnico especializado (ITEM 15), onde o pagamento será mensal.
8.2 Para fins de pagamento, a CONTRATADA deverá ainda, apresentar juntamente com a nota fiscal, as certidões de regularidade fiscal e trabalhista.
8.3 O pagamento será efetuado mediante a apresentação da Fatura/Nota Fiscal junto ao Protocolo da CONTRATANTE ou envio através de e-mail para logistica@prodepa.pa.gov.br, tendo como complemento a obrigatoriedade de envio de suas certidões fiscais e relatório de medição do período. Devendo ser devidamente atestada pelo Fiscal de Contrato.
8.4 O prazo máximo para a entrega dos itens pela CONTRATADA será de até 90 (noventa) dias corridos, contados a partir da data de solicitação;
8.5 A CONTRATANTE tem até 30 (trinta) dias corridos para emitir o Termo de Aceite Definitivo após o recebimento dos produtos ou serviços.
8.6 A CONTRATANTE tem até 15 (quinze) dias corridos para emitir o ateste da Nota Fiscal a emissão o Termo de Aceite Definitivo
8.7 A CONTRATANTE realizará o pagamento das Notas Fiscais em até 30 (trinta) dias corridos após o ateste da mesma.

3.3. Validade da Proposta

Os termos e condições desta proposta são válidos por um período de 90 (noventa) dias a contar da data de sua apresentação.

3.4. Observações e Declarações:

Os preços incluem taxas, impostos, seguros pertinentes, custos diretos e indiretos, tributos, encargos sociais, tributários, trabalhistas e previdenciários, seguros, taxas, lucro e outros necessários ao cumprimento integral do objeto.

Todos os serviços, peças, assessórios e equipamentos de reposição que, embora não mencionados, sejam necessários para a perfeita e integral execução do serviço.

4.Informações Complementares

4.1. Proponente

Razão Social: Alltech Soluções em Tecnologia Ltda.

CNPJ: 21.547.011/0001-66

Endereço: SCN Quadra 01 Bloco F – Salas 802 a 810 – Ed. America Office Tower

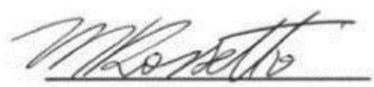
– Brasilia, DF

E-mail:mrossetto@alltechsolucoes.com.br
Telefone: (61) 3344-0236 (61) 99818-3179.
Inscrição Estadual: 07.704.559/001-89
Optante pelo Simples: Não.

Dados do Representante Legal da Empresa para assinatura do Contrato:
Nome: Murilo Rossetto
CPF/MF: 036.031.821-54
E-mail: mrossetto@alltechsolucoes.com.br
Cargo/Função: Diretor

4.2. Operação de Crédito

Banco do Brasil S.A.
Agência: 3382-0 C/C: 6734-2
Brasília, DF



Murilo Rossetto
Representante Legal
Alltech Soluções em Tecnologia Ltda