DEFENSORIA PÚBLICA DO AMAPÁ
Rua Eliezer Levy, Nº 1157 - Bairro Centro - CEP 68900-083 - Macapá - AP - defensoria.ap.def.br

TERMO DE REFERÊNCIA

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Definição do objeto

1.1.1. Registro de Preços para eventual Contratação de solução de segurança de rede do tipo **Next Generation Firewall (NGFW)**[1], compreendendo o fornecimento de licenças, equipamentos, software, garantia, suporte técnico especializado, atualizações, manutenção corretiva e evolutiva, bem como os serviços de instalação, configuração, migração de ambiente, treinamento e operação assistida, pelo período de **60 (sessenta) meses**, visando assegurar a proteção da infraestrutura tecnológica, a disponibilidade dos serviços de rede, o controle de acessos, a prevenção e detecção de ameaças cibernéticas e o atendimento às necessidades de segurança da informação da instituição.

1.2. Natureza do objeto

1.2.1. Bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado;

1.2.2. Fornecimento e prestação de serviço associado

1.3. Da origem da demanda e do catálogo eletrônico de padronização

1.3.1. Esta peça foi elaborada com base no §1º, art. 18, da Lei Federal nº 14.133, de 2021, na Portaria nº 38, de 2024 - DPE/AP, desenvolvida no Sistema Eletrônico de Informações - SEI, de acordo com o art. 1º, §1º, da Portaria 170, de 2025 - DPE/AP, em conformidade com a Instrução Normativa nº 03, de 2024 - DPE/AP, com base no despacho SEI(0214917) **Prosseguimento do Processo Licitatório**: Autoriza-se o prosseguimento do processo licitatório referente à **contratação n.º 27/2026 do PCA/2026 – TIC - Infraestrutura de Segurança - Firewall**, prevista no PCA/2026, dando-se continuidade à execução do calendário aprovado pelo Defensor Público-Geral, **ID do item** n.º **159** - *Link de acesso ao PCA/2026 (APROVADO)*, torna-se necessário dar início à fase de planejamento da respectiva contratação, nos moldes do artigo 18 da referida Lei.

1.3.2. Este instrumento contém as especificações padronizadas para o objeto em tela, atendendo aos quesitos do catálogo eletrônico de padronização do Poder Executivo Federal (art. 6º, §2º, da Portaria nº 38, de 2024 – DPE/AP), conforme códigos do CATMAT e CATSER – Catálogo de Materiais e Serviços, já descritos no quadro apresentado no subitem anterior.

1.4. Quantitativos

1.4.1. Este processo será conduzido por meio de um pregão eletrônico em conjunto com o sistema de registro de preços, o que permite uma aquisição mais eficiente e transparente, assegurando a melhor relação custo-benefício para a administração pública e possibilitando ajustes conforme a necessidade, sua justificativa foi demonstrado no item 9 do Estudo Técnico Preliminar.

1.4.2. A adoção do Sistema de Registro de Preços (SRP) para a presente contratação encontra amparo nos arts. 82 a 86 da Lei Federal nº 14.133, de 1º de abril de 2021, bem como no art. 3º, incisos I e II, da Portaria nº 46, de 10 de janeiro de 2024, que regulamenta a utilização do SRP no âmbito desta Instituição. A utilização do procedimento mostra-se adequada em razão da necessidade de contratações frequentes decorrentes das características do objeto, bem como da conveniência da aquisição parcelada dos bens e serviços acessórios associados, possibilitando que a Administração realize as contratações de acordo com a efetiva necessidade institucional.

1.4.3. A presente contratação será executada de forma parcelada, mediante a emissão de ordens de fornecimento e/ou ordens de serviço, conforme a necessidade da Defensoria Pública do Estado do Amapá. A remuneração será realizada com base nos preços unitários registrados para cada item, considerando-se os quantitativos efetivamente fornecidos ou os serviços efetivamente executados, observadas as condições e os requisitos estabelecidos neste Termo de Referência.

1.4.4. No Sistema Compras.gov.br, as propostas e os lances serão registrados de forma individualizada para cada item,

conforme a operacionalização da plataforma, sendo o julgamento realizado pelo critério de menor preço por item, observados os requisitos de habilitação, aceitabilidade e exequibilidade dos preços.

1.4.5.O quantitativo indicado na tabela a seguir representa uma estimativa das quantidades que a Defensoria Pública do Estado do Amapá poderá utilizar ao longo da vigência da Ata de Registro de Preços e/ou da execução contratual, não constituindo obrigação de contratação integral dos quantitativos estimados, ficando as solicitações condicionadas à efetiva necessidade da Administração.

TABELA DE QUANTITATIVOS

GRUPO	ITEM	DESCRIÇÃO	UNIDADE	QUANT. MÍNIMA	QUANT. MÁXIMA	VALOR UNITÁRIO	VALOR TOTAL
1	**1**	Solução de proteção de perímetro com NGFW (Next Generation Firewall) "tipo 01", com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses. (CATMAT/ CATSER 609340).	UNIDADE	1	4	R$ 1.424.738,94	R$ 5.698.955,76
	2	Solução de proteção de perímetro com NGFW (Next Generation Firewall) "tipo 02", com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses.(CATMAT/ CATSER 609340).	UNIDADE	1	4	R$ 429.734,95	R$ 1.718.939,80
	3	Solução de proteção de perímetro com NGFW (Next Generation Firewall) "tipo 03", com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses.(CATMAT/	UNIDADE	1	10	R$ 182.829,17	R$ 1.828.291,70

	CATSER 609340).					
4	Solução de proteção de perímetro com NGFW (Next Generation Firewall) "tipo 04", com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses.(CATMAT/ CATSER 609340).	UNIDADE	1	10	R$ 125.813,57	R$ 1.258.135,70
5	Solução de proteção de perímetro com NGFW (Next Generation Firewall) "tipo 05", com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses.(CATMAT/ CATSER 609340).	UNIDADE	1	10	R$ 92.594.14	R$ 925.941,40
6	Solução de GESTÃO DE LOGS E RELATÓRIOS de ambiente unificado de NGFW (Next Generation Firewall), com log/ rate de 25GB/Dia, com implantação, garantia do fabricante, repasse de conhecimento e suporte, pelo período de 60 meses. (CATMAT/ CATSER 27472).	UNIDADE	1	2	R$ 151.976,78	R$ 303.953,56
7	Solução de GESTÃO CENTRALIZADA de ambiente unificado de NGFW (Next Generation Firewall), com	UNIDADE	1	4	R$ 71.669,21	R$ 286.676,84

		implantação, garantia do fabricante, repasse de conhecimento e suporte, para até 10 dispositivos físicos, pelo período de 60 meses. (CATMAT/ CATSER 27472).					
	8	Unidade de Serviços Técnicos - USTs . (CATMAT/ CATSER 27057).	HORAS	1	4000	R$ 449,47	R$ 1.797.880,00
	TOTAL :						**R$ 13.818.774,76**

1.5. Do registro de preço e sua prorrogação

Do Registro de Preços

1.5.1. O uso do Sistema de Registro de Preços (SRP) para o presente certame fundamenta-se nos arts. 82 a 86 da Lei Federal nº 14.133, de 2021, no art. 3º, incisos I e II, da Portaria nº 46, de 2024 – DPE/AP, e no art. 3º, incisos I e II, do Decreto Federal nº 11.462, de 2023, em virtude de tratar-se de contratação destinada ao fornecimento de bens permanentes de tecnologia da informação, com prestação de serviços acessórios associados, cujas características demandam contratações frequentes e fornecimento parcelado, permitindo que a Administração realize as aquisições conforme a necessidade institucional e a disponibilidade orçamentária, sem a obrigatoriedade de contratação imediata do quantitativo máximo estimado.

1.5.2.A adoção do procedimento auxiliar de Sistema de Registro de Preços visa maior celeridade nas contratações, redução da quantidade de licitações, possibilidade de utilização da Ata por outros órgãos públicos e menores preços pelo efeito da economia de escala.

1.5.3. Por força do art. 83, da Lei Federal no 14.133, de 2021, art. 20, da Portaria no 46, de 2024 - DPE/AP e art. 21 do Decreto Federal no 11.462, de 2023, a existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obriga a Defensoria Pública a contratar, facultada a realização de licitação ou de contratação direta específica para o atendimento da demanda, desde que devidamente justificado.

1.5.4. A justificativa da utilização do sistema de registro de preços para o presente objeto consta no item 9.7 do

Estudo Técnico Preliminar de forma mais detalhada.

Da Ata de Registro de Preços

1.5.4. Após a homologação do certame, o licitante adjudicatário será convocado para assinar a Ata de Registro de Preços no prazo de 05 (cinco) dias úteis, podendo este prazo ser prorrogado uma vez, por igual período, mediante solicitação justificada e aceita pela Administração. A recusa injustificada em assinar o documento dentro do prazo estabelecido caracteriza o descumprimento total da obrigação assumida, sujeitando o licitante à perda do direito à contratação e à aplicação das sanções previstas na Lei nº 14.133, de 2021, nos termos do art. 18, da Portaria nº 46, de 2024 – DPE/AP, em conformidade com o art. 19, do Decreto Federal nº 11.462, de 2023.

1.5.5.O prazo de vigência da Ata de Registro de Preços será de 01 (um) ano, contado do primeiro dia útil subsequente à data da divulgação no PNCP, e poderá ser prorrogada, por igual período, desde que comprovado o preço vantajoso, na forma do art. 84, da Lei Federal nº 14.133, de 2021, art. 21 da Portaria nº 46, de 2024 - DPE/AP e art. 23, do Decreto Federal nº 11.462, de 2023.

1.5.6. Em hipótese de prorrogação da Ata de Registro de Preços, o quantitativo originalmente registrado poderá ser restabelecido, nos termos do art. 1º, da Portaria nº 823, de 2025 - DPE/AP, que alterou dispositivos (at. 21 e art. 22) da Portaria nº 46/2024 - DPE/AP, responsável por regulamentar os artigos 82 a 86 da Lei Federal nº 14.133/2021.

1.5.7. Será admitida a adesão à Ata de Registro de Preços decorrente da licitação, nos termos do art. 31, da portaria no 46, de 2024 - DPE/AP e art. 31, §2º, do Decreto Federal no 11.462, de 2023.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. A Defensoria Pública do Estado do Amapá desempenha papel essencial na promoção do acesso à justiça e na defesa dos direitos da população hipossuficiente, realizando diariamente o tratamento de informações sensíveis, dados pessoais, processos judiciais e administrativos que demandam elevado nível de proteção e disponibilidade.

2.2. Nesse contexto, a segurança da informação constitui elemento estratégico para a continuidade das atividades institucionais, tornando indispensável a manutenção e o fortalecimento dos mecanismos de proteção da infraestrutura tecnológica da instituição.

2.3. Atualmente, a Defensoria Pública do Estado do Amapá utiliza solução de segurança baseada em firewall da fabricante WatchGuard, cuja contratação vigente contemplou exclusivamente o fornecimento das licenças de subscrição e suporte pelo período de 12 (doze) meses.

2.4. As licenças atualmente em uso possuem vigência até outubro de 2026. Após esse período, os equipamentos deixarão de receber atualizações de assinaturas de segurança, inteligência contra ameaças, suporte técnico especializado e demais serviços essenciais para o adequado funcionamento da solução de proteção perimetral.

2.5. A interrupção desses serviços poderá comprometer significativamente a capacidade de prevenção, detecção e resposta a incidentes de segurança cibernética, expondo a rede institucional a vulnerabilidades, acessos não autorizados, vazamento de informações, indisponibilidade de sistemas e outras ameaças que possam impactar diretamente a prestação dos serviços da Defensoria Pública.

2.6. Além da necessidade de garantir a continuidade da proteção atualmente existente, observa-se que a crescente digitalização dos serviços públicos, a ampliação dos sistemas corporativos, a utilização de serviços em nuvem, o aumento do volume de dados trafegados e a evolução constante das ameaças cibernéticas exigem a adoção de uma solução de segurança mais abrangente e moderna.

2.7. Nesse cenário, torna-se necessária a contratação de uma solução de Next Generation Firewall (NGFW), capaz de oferecer recursos avançados de proteção, tais como inspeção profunda de pacotes (Deep Packet Inspection)[2], sistema de prevenção de intrusão (IPS)[3], controle de aplicações, filtragem web, proteção contra malware, detecção de ameaças avançadas, inspeção de tráfego criptografado, inteligência de ameaças em tempo real, estabelecimento de redes privadas virtuais (VPN)[4] seguras e mecanismos de alta disponibilidade.

2.8. A adoção de uma solução NGFW permitirá à Defensoria Pública aprimorar sua postura de segurança, ampliando a capacidade de identificação, bloqueio e mitigação de ataques cibernéticos cada vez mais sofisticados, reduzindo riscos operacionais e fortalecendo a proteção dos ativos tecnológicos institucionais.

2.9. A contratação também visa assegurar a continuidade dos serviços de suporte técnico, garantia do fabricante, atualizações de software e assinaturas de segurança durante todo o período contratual, garantindo

que a solução permaneça atualizada frente às novas vulnerabilidades e vetores de ataque identificados no cenário global de segurança da informação.

2.10. A presente contratação está alinhada aos princípios da eficiência, continuidade do serviço público, planejamento e gestão de riscos, contribuindo para a manutenção da disponibilidade, integridade, confidencialidade e autenticidade das informações sob responsabilidade da Defensoria Pública do Estado do Amapá.

2.11. Adicionalmente, a contratação atende às diretrizes estabelecidas pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)[5], especialmente quanto ao dever de adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

2.12. Destaca-se, por fim, que o objeto da presente contratação não se enquadra na categoria de bens e serviços de luxo, nos termos do art. 4º, inciso III, da Portaria nº 32/2024 – DPE/AP, tratando-se de solução essencial à continuidade das atividades institucionais e à proteção dos ativos de tecnologia da informação da Defensoria Pública do Estado do Amapá.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

3.1. As informações detalhadas acerca da descrição completa da solução encontram-se anexas a este Termo de Referência (**APÊNDICE I - ANEXO I - ESPECIFICAÇÃO TÉCNICA DOS EQUIPAMENTOS)**, constituindo parte integrante do presente documento.

4. DESCRIÇÃO E REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. Garantir a continuidade, disponibilidade e segurança dos serviços tecnológicos que suportam as atividades finalísticas da Defensoria Pública do Estado do Amapá, contribuindo para a promoção do acesso à justiça e a proteção dos direitos do cidadão.

4.1.2. Assegurar a proteção dos dados institucionais, informações processuais, administrativas e pessoais tratados pela Defensoria Pública, em conformidade com as boas práticas de segurança da informação e com a legislação vigente.

4.1.3. Fortalecer a governança de Tecnologia da Informação por meio da adoção de solução de segurança capaz de proporcionar controle, monitoramento, rastreabilidade e gestão centralizada do ambiente de rede institucional.

4.1.4. Aprimorar os mecanismos de prevenção, detecção e resposta a incidentes de segurança cibernética, reduzindo riscos relacionados a acessos não autorizados, vazamento de dados, ataques virtuais e indisponibilidade de serviços.

4.1.5. Garantir a manutenção dos níveis de proteção atualmente existentes e prover evolução tecnológica da infraestrutura de segurança perimetral da instituição, considerando o encerramento da vigência das licenças da solução atualmente utilizada.

4.1.6. Possibilitar a implementação de recursos avançados de segurança, incluindo inspeção de tráfego, prevenção de intrusões, controle de aplicações, proteção contra malware, filtragem de conteúdo e monitoramento de ameaças em tempo real.

4.1.7. Assegurar suporte técnico especializado, atualizações de software, assinaturas de segurança e garantia da solução durante toda a vigência contratual, preservando a efetividade da proteção contra ameaças cibernéticas emergentes.

4.1.8. Proporcionar escalabilidade e capacidade de crescimento da infraestrutura de segurança, acompanhando a expansão dos serviços digitais, sistemas corporativos e demandas tecnológicas da Defensoria Pública do Estado do Amapá.

4.2. Requisitos Legais

4.2.1. O presente processo de contratação deve estar aderente à Constituição da República Federativa do Brasil de 1988, Lei nº14.133/21 (Lei de Licitações e Contratos Administrativos), Portaria nº 38, de 10 de Janeiro de 2024 (Regulamenta a elaboração do Termo de Referência – TR e alterações, no âmbito da Defensoria Pública do Estado do Amapá).

4.3. Requisitos Temporais

4.3.1. A entrega deverá ser realizada nas dependências da Defensoria Pública do Estado do Amapá (Avenida Raimundo Alvares da Costa, nº 676, Bairro Centro, Macapá - AP, CEP: 68.900-074 - Anexo II), compreendendo transporte, descarregamento, conferência e demais procedimentos necessários ao recebimento definitivo, segunda a sexta-feira, das 07h30 às 16h30, no expediente da instituição, conforme a Portaria nº 412, de 8 de maio de 2024, e suas alterações, durante a execução do contrato.

4.3.2. A data de Entrega dos Produtos (prazo de até 30 dias)

4.3.2.1. Confirmada a demanda, a CONTRATADA deverá realizar a entrega dos produtos e/ou a execução dos serviços no prazo de até 30 (trinta) dias, contado na forma estabelecida neste Termo de Referência.

4.3.2.2. O prazo de entrega poderá ser prorrogado, por igual período, mediante solicitação formal e devidamente fundamentada da CONTRATADA, quando ocorrerem fatos supervenientes, imprevisíveis ou de consequências incalculáveis, alheios à sua vontade, que comprovadamente impeçam ou dificultem o cumprimento do prazo originalmente estabelecido.

4.3.2.3. A solicitação de prorrogação deverá ser apresentada pela CONTRATADA tão logo tenha conhecimento do fato que possa comprometer o cumprimento do prazo, acompanhada de documentação e elementos comprobatórios suficientes para demonstrar a ocorrência, a relação de causalidade com o atraso e a impossibilidade ou dificuldade de cumprimento do prazo original.

4.3.2.4. .A concessão da prorrogação não será automática, ficando condicionada à análise e manifestação da CONTRATANTE, que avaliará a pertinência dos fatos alegados, a documentação apresentada e o impacto sobre o cumprimento das obrigações contratuais.

4.3.2.5. A prorrogação somente será admitida quando ficar comprovado que o evento não decorreu de ação ou omissão da CONTRATADA e que foram adotadas, por esta, todas as medidas razoavelmente disponíveis para evitar ou reduzir os efeitos do fato superveniente sobre o prazo de entrega.

4.3.2.6. Consideram-se, para fins deste dispositivo, sem prejuízo de outras situações devidamente comprovadas, eventos externos que possam afetar diretamente o fornecimento, tais como fatos da natureza, determinações de autoridades públicas, interrupções relevantes de transporte ou logística, indisponibilidade comprovada de componentes ou matérias-primas decorrente de eventos excepcionais, situações de força maior ou caso fortuito e outros acontecimentos alheios à esfera de controle da CONTRATADA.

4.3.2.7. A eventual concessão da prorrogação deverá ser formalizada pela CONTRATANTE, não implicando, por si só, alteração das demais obrigações, condições, preços ou quantitativos estabelecidos na contratação.

4.4. Requisitos Sociais, Ambientais e Culturais

4.4.1. O art. 5º e o art.11, inciso IV, da Lei Federal nº 14.133/2021 destacam a importância da sustentabilidade como um dos princípios fundamentais a serem observados nas contratações públicas. Isso significa que a Administração deve buscar contratar serviços e adquirir produtos de forma a promover o desenvolvimento sustentável, considerando aspectos ambientais, sociais e econômicos, como prevê o parágrafo único do art. 10, da Portaria nº 40/2024 - DPE/AP.

4.4.2. Assim, a futura Contratada deverá respeitar a legislação vigente e as normas técnicas, atendendo aos critérios de sustentabilidade eventualmente inseridos na descrição do objeto e no Guia Nacional de Contratações Sustentáveis - 8ª Edição, Outubro/2025, na Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010, regulamentado pelo Decreto nº 10.936/2022).

4.4.3. Todos os materiais devem ser constituídos e embalados com critérios socioambientais vigentes decorrentes da Lei nº 6.938/81 e regulamentos, com os respectivos registros e comprovação ambientais, além de atentar para as exigências da Política de Resíduos Sólidos (Lei nº 12.305/2010 e Decreto nº 10.936/2022).

4.4.4. Seguindo a lógica do item 4.4.1., importante que também se atenda a sustentabilidade social, no tocante ao respeito aos direitos trabalhistas, ao exigir que a Contratada demonstre sua regularidade, comprovando o cumprimento de suas obrigações trabalhistas, para a devida habilitação e posterior execução do contrato; e a dimensão econômica, ao buscar garantir transparência e integridade nos processos de compras públicas desenvolvidos por esta Defensoria, assegurando a imparcialidade nas decisões.

4.4.5. Por fim, deverá ser observado, no que couber, as disposições estabelecidas nos itens 5.1, 5.2 e 5.3 da Portaria nº 393/2024 - DPE/AP, que institui a Defensoria Verde - plano de sustentabilidade e uso racional dos recursos públicos.

4.5. Requisito de Tecnologia para Infraestrutura de Firewall

4.5.1. A contratação de solução de Next Generation Firewall (NGFW) exige a observância de requisitos tecnológicos capazes de garantir a proteção da infraestrutura de rede da Defensoria Pública do Estado do Amapá diante das atuais ameaças cibernéticas. A solução deverá disponibilizar recursos avançados de segurança integrados em uma plataforma única, contemplando, no mínimo, sistema de prevenção e detecção de intrusões (IPS/IDS), controle de aplicações, filtragem de conteúdo web, proteção contra malware, inspeção profunda de pacotes (Deep Packet Inspection), inteligência de ameaças em tempo real e mecanismos de proteção contra ataques avançados.

4.5.2. A solução deverá permitir a inspeção e análise do tráfego criptografado por meio de SSL/TLS Inspection[6], possibilitando a identificação de ameaças ocultas em conexões seguras, sem comprometer o desempenho da rede institucional.

4.5.3. Os equipamentos e licenças fornecidos deverão possuir capacidade compatível com o ambiente tecnológico da Defensoria Pública, considerando o volume atual e projetado de tráfego de dados, usuários, conexões simultâneas e serviços disponibilizados pela instituição, garantindo níveis adequados de desempenho, disponibilidade e segurança.

4.5.4. A solução deverá oferecer suporte à criação e gerenciamento de redes privadas virtuais (VPN), incluindo os protocolos IPSec e SSL VPN ou equivalentes, permitindo a comunicação segura entre unidades da instituição, usuários remotos e ambientes externos autorizados.

4.5.5. Deverá ser disponibilizada plataforma de gerenciamento centralizado, preferencialmente baseada em nuvem ou solução equivalente, permitindo a administração unificada de políticas de segurança, monitoramento em tempo real, geração de relatórios, auditoria de eventos, controle de acessos e gerenciamento dos dispositivos integrantes da solução.

4.5.6. A solução deverá contemplar mecanismos avançados de autenticação de usuários e dispositivos, integração com serviços de diretório corporativo, controle granular de acessos e aplicação de políticas de segurança baseadas em perfis, grupos ou contextos operacionais.

4.5.7. Os equipamentos deverão suportar recursos de alta disponibilidade (High Availability - HA)[7], redundância e recuperação de falhas, garantindo a continuidade dos serviços críticos mesmo em situações de indisponibilidade de componentes da infraestrutura.

4.5.8. A solução deverá possuir características de escalabilidade que permitam sua expansão futura, acompanhando o crescimento da infraestrutura tecnológica da Defensoria Pública sem a necessidade de substituição integral dos equipamentos ou perda significativa de desempenho.

4.5.9. Durante toda a vigência contratual, deverão ser disponibilizados suporte técnico especializado, garantia do fabricante, atualizações de firmware, correções de segurança, atualizações das bases de assinaturas de ameaças, inteligência de segurança e demais componentes necessários para manutenção da efetividade da proteção cibernética.

4.5.10. A solução deverá disponibilizar recursos de monitoramento, correlação de eventos, geração de logs, relatórios gerenciais e integração com ferramentas de análise e resposta a incidentes, contribuindo para o fortalecimento da governança de segurança da informação da instituição.

4.5.11. Os componentes da solução deverão estar em linha de fabricação e comercialização pelo fabricante durante toda a vigência contratual, assegurando suporte contínuo, disponibilidade de atualizações e compatibilidade tecnológica com as necessidades institucionais.

4.5.12. A solução contratada deverá atender às boas práticas e normas aplicáveis à segurança da informação, proteção de dados pessoais e continuidade dos serviços públicos, contribuindo para a preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações sob responsabilidade da Defensoria Pública do Estado do Amapá.

4.6. Requisitos de Instalação e Configuração

4.6.1. A solução de Next Generation Firewall (NGFW) deverá ser instalada e configurada de forma a atender às necessidades operacionais, de desempenho e de segurança da Defensoria Pública do Estado do Amapá,

observando as boas práticas de mercado e as diretrizes institucionais de Tecnologia da Informação e Segurança da Informação

4.6.2. As atividades de implantação serão executadas pela equipe técnica da Defensoria Pública do Estado do Amapá, com o apoio técnico especializado da empresa contratada, que deverá disponibilizar profissionais qualificados para orientar, acompanhar e prestar suporte durante todas as etapas de instalação, configuração, migração e entrada em operação da solução.

4.6.3. Caberá à contratada fornecer a documentação técnica necessária, orientações de instalação, procedimentos recomendados pelo fabricante e suporte consultivo para garantir a correta implementação da solução no ambiente institucional.

4.6.4. A configuração deverá contemplar, entre outros aspectos, a definição de políticas de segurança, regras de firewall, segmentação de rede, configuração de VPNs, integração com serviços de autenticação, proteção contra ameaças, monitoramento, geração de logs e demais funcionalidades contratadas, de acordo com os requisitos definidos pela Defensoria Pública.

4.6.5. Sempre que necessário, a contratada deverá prestar apoio técnico na migração das configurações atualmente existentes para a nova solução, visando reduzir impactos operacionais e assegurar a continuidade dos serviços durante o processo de transição.

4.6.6. A implantação deverá ser realizada de forma planejada, minimizando indisponibilidades dos serviços institucionais e preservando a integridade das informações e dos ambientes tecnológicos existentes.

4.6.7. Após a conclusão da instalação e configuração, a contratada deverá validar, em conjunto com a equipe técnica da Defensoria Pública, o correto funcionamento da solução, realizando testes operacionais e de conectividade que comprovem a efetividade dos recursos de segurança implementados.

4.6.8. A contratada deverá disponibilizar suporte técnico durante o período inicial de operação assistida, auxiliando a equipe da Defensoria Pública na resolução de eventuais inconsistências, ajustes de configuração e otimização do ambiente implantado.

4.6.9. Ao término da implantação, deverão ser fornecidos documentos contendo as configurações implementadas, topologia da solução, procedimentos de administração e demais informações necessárias para a adequada gestão e manutenção do ambiente pela equipe técnica da Defensoria Pública do Estado do Amapá.

4.7. Requisitos de Repasse de Conhecimento (operação assistida) e suporte especializado.

4.7.1. A CONTRATADA deverá realizar o repasse de conhecimento à equipe indicada pela CONTRATANTE, após a conclusão da implantação e/ou migração das soluções, com o objetivo de proporcionar aos usuários e administradores os conhecimentos necessários para a adequada operação, administração, configuração e utilização da solução contratada.

4.7.2. O repasse de conhecimento deverá ser realizado por meio de aulas ministradas por profissionais devidamente capacitados e com conhecimento comprovado sobre as soluções implantadas, contemplando abordagem teórica e prática, demonstração das funcionalidades e execução orientada dos principais procedimentos relacionados ao ambiente contratado.

4.7.3. A capacitação deverá possuir duração mínima de 8 (oito) horas, podendo ser realizada de forma presencial, remota ou híbrida, conforme definido pela CONTRATANTE, e deverá abranger, no mínimo:

4.7.3.1. Visão geral da arquitetura e dos componentes que integram a solução;

4.7.3.2. Apresentação das funcionalidades disponibilizadas e dos recursos implementados;

4.7.3.3. Operação e utilização das funcionalidades da solução;

4.7.3.4. Procedimentos de administração e gerenciamento do ambiente;

4.7.3.5. Configuração e parametrização dos componentes da solução;

4.7.3.6. Procedimentos para inclusão, alteração, exclusão e gerenciamento de usuários, perfis, permissões e demais elementos administrativos, quando aplicável;

4.7.3.7. Procedimentos de monitoramento, acompanhamento e verificação do funcionamento da solução;

4.7.3.8. Procedimentos básicos para identificação e tratamento de falhas e ocorrências;

4.7.3.9. Procedimentos de manutenção, atualização e demais rotinas necessárias à adequada administração da solução;

4.7.3.10. Boas práticas de utilização, administração, segurança e continuidade operacional;

4.7.3.11. Orientações quanto aos procedimentos para abertura, acompanhamento e escalonamento de chamados junto à CONTRATADA e/ou aos fabricantes, quando aplicável.

4.7.4. As aulas deverão ser estruturadas de forma a contemplar diferentes níveis de conhecimento, considerando, quando aplicável, conteúdos destinados aos usuários da solução e conteúdos específicos para os profissionais responsáveis por sua administração, configuração e gerenciamento.

4.7.5. A CONTRATADA deverá fornecer material de apoio para acompanhamento das aulas e posterior consulta pela CONTRATANTE, em formato digital, contendo, no mínimo, manuais, apresentações, guias de operação, procedimentos administrativos, instruções de configuração e demais materiais necessários à utilização e administração da solução.

4.7.6. Além das aulas, a CONTRATADA deverá disponibilizar videoaulas gravadas referentes aos principais conteúdos apresentados durante a capacitação, de modo a permitir a revisão dos procedimentos, a capacitação de novos usuários e a consulta posterior pela equipe da CONTRATANTE.

4.7.6.1. As videoaulas deverão ser disponibilizadas em meio eletrônico ou plataforma indicada pela CONTRATADA, com acesso garantido à CONTRATANTE durante todo o período de vigência do licenciamento da solução, sem custos adicionais.

4.7.6.2. As videoaulas deverão apresentar conteúdo compatível com a versão da solução efetivamente implantada e contemplar, sempre que aplicável, demonstrações práticas dos procedimentos de operação, administração e configuração.

4.7.7. A CONTRATADA deverá fornecer documentação completa e atualizada da solução implantada, em formato digital, abrangendo, no mínimo, a documentação técnica, operacional e administrativa necessária para sua adequada utilização e gestão pela CONTRATANTE.

4.7.7.1. A documentação deverá contemplar, quando aplicável:

a) descrição geral e arquitetura da solução;

b) relação dos componentes, módulos e funcionalidades implantados;

c) configurações e parametrizações realizadas;

d) procedimentos de instalação, configuração e administração;

e) procedimentos de operação e utilização;

f) procedimentos de gerenciamento de usuários, perfis e permissões;

g) procedimentos de monitoramento e acompanhamento;

h) procedimentos de manutenção e atualização;

i) procedimentos para identificação e tratamento de falhas;

j) informações sobre integrações, interfaces, APIs e demais mecanismos de comunicação com outros sistemas, quando aplicável;

k) procedimentos de backup, restauração, contingência e recuperação, quando aplicável;

l) recomendações e boas práticas para operação e administração;

m) demais informações necessárias à continuidade e adequada gestão da solução pela CONTRATANTE.

4.7.8. A documentação fornecida deverá refletir as configurações e características da solução efetivamente implantada e/ou migrada, não sendo admitida a entrega de documentação genérica que não corresponda ao ambiente disponibilizado à CONTRATANTE.

4.7.9. Sempre que houver alteração relevante na solução, em suas funcionalidades, configurações ou procedimentos de administração, a CONTRATADA deverá manter atualizados os materiais de apoio e a documentação correspondente, durante o período de vigência da contratação, quando a alteração decorrer de atualização, evolução ou manutenção realizada no âmbito dos serviços contratados.

4.7.10. A CONTRATADA deverá disponibilizar à CONTRATANTE os materiais de capacitação, videoaulas e documentação em formato digital que permita sua consulta, armazenamento e utilização posterior, sem restrições que impeçam o acesso pela equipe da CONTRATANTE durante a vigência contratual.

4.7.11. O conteúdo disponibilizado deverá ser suficiente para permitir que a equipe técnica e os usuários indicados pela CONTRATANTE adquiram autonomia para a execução das atividades ordinárias de operação, utilização e administração da solução, sem prejuízo do suporte técnico especializado contratado.

4.7.12. Ao término do repasse de conhecimento, a CONTRATADA deverá disponibilizar à CONTRATANTE a relação dos conteúdos ministrados, os materiais utilizados nas aulas, as videoaulas e a documentação completa da solução, ficando todos esses materiais disponíveis para consulta posterior.

4.7.13. O repasse de conhecimento, o fornecimento dos materiais de apoio, das videoaulas e da documentação completa constituem obrigações integrantes da implantação da solução, não podendo sua execução ou disponibilização resultar em cobrança adicional à CONTRATANTE.

4.7.14. A CONTRATANTE poderá solicitar esclarecimentos complementares relacionados aos conteúdos ministrados durante o repasse de conhecimento, cabendo à CONTRATADA prestar as orientações necessárias para assegurar a adequada compreensão dos procedimentos apresentados.

4.8. Requisitos de Proteção de Dados

4.8.1.Em conformidade com a **Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD)**, a **Lei Federal nº 12.527/2011 (Lei de Acesso à Informação)**, a **Lei Federal nº 14.129/2021 (Lei do Governo Digital)** e as **Portarias DPG nº 510 e nº 511, de 23 de maio de 2025**, da Defensoria Pública do Estado do Amapá, a contratada deverá garantir o tratamento adequado de dados pessoais, observando os princípios da finalidade, necessidade, segurança, transparência, prevenção e responsabilização, conforme disposto nos artigos 6º e 7º da LGPD. O compartilhamento de dados deverá ocorrer apenas em ambientes seguros e exclusivamente quando estritamente necessário à execução dos serviços contratados, nos termos do artigo 26 da LGPD e do artigo 2º, inciso IX, da Portaria DPG nº 511/2025.

4.8.2.As informações pessoais e sigilosas devem ser protegidas quanto à sua confidencialidade, integridade, autenticidade e disponibilidade, conforme o artigo 3º, incisos II e III, da Portaria DPG nº 510/2025. A solução implementada deverá adotar controles de acesso baseados em perfis de usuários, com autenticação individualizada e registro de logs, garantindo a rastreabilidade e auditabilidade das ações, em atenção ao artigo 46 da LGPD. O tratamento dos dados deverá observar os princípios da transparência ativa e da prestação de contas, assegurando o acesso do cidadão às informações públicas, sem prejuízo da proteção de dados sensíveis, nos termos do artigo 7º da Lei nº 12.527/2011 e do artigo 29 da Lei nº 14.129/2021.

4.8.3.A coleta de dados pessoais deverá ser limitada à finalidade específica, mediante consentimento do titular, quando exigido pela legislação, conforme estabelecido nos artigos 7º e 8º da LGPD. Nos pedidos de abertura de bases de dados, deverá ser assegurada, sempre que solicitada, a preservação da identidade do requerente, nos termos do artigo 10, §3º, da Portaria DPG nº 511/2025. A contratada deverá manter plano de contingência com políticas de backup e recuperação de dados que garantam a continuidade dos serviços e a proteção das informações em caso de falha ou incidente de segurança.

4.8.4.A solução deverá incluir mecanismos de auditoria e registro de eventos que permitam a responsabilização por acessos e manipulação indevida de dados, conforme o artigo 6º, inciso X, da LGPD. Por fim, é exigida a capacitação continuada dos agentes públicos envolvidos no tratamento de dados, com vistas à conformidade com a legislação vigente e ao uso adequado das tecnologias digitais, conforme previsto no artigo 2º, inciso XVIII, da Portaria DPG nº 511/2025.

4.9. Requisitos de Garantia

4.9.1. Considerando a natureza da contratação e o regime jurídico aplicável às contratações realizadas pela Administração Pública, estabelece-se que a garantia dos bens e serviços contratados será regida primariamente pela Lei Federal nº 14.133/2021 e pelas disposições contratuais, aplicando-se o Código de Defesa do Consumidor – CDC, de forma subsidiária e quando compatível com a relação jurídica estabelecida.

4.9.2. Esclarece-se, ainda, que o prazo de 90 (noventa) dias previsto no CDC constitui prazo legal mínimo aplicável às hipóteses por ele abrangidas, não se confundindo nem substituindo a garantia contratual estabelecida para a presente contratação. A garantia contratual possui natureza complementar e deverá observar os prazos e condições definidos no instrumento convocatório, no contrato e nas especificações do objeto, prevalecendo, quando mais favoráveis à Administração, as condições de garantia expressamente estabelecidas pela contratação.

- **Prazo Legal (CDC - Art. 26):**

- Para **vícios aparentes ou de fácil constatação** em bens duráveis (como equipamentos de data center), o prazo de reclamação é de **90 (noventa) dias**, contados a partir da entrega efetiva do produto ou término da execução dos serviços.
- Para **vícios ocultos** (aqueles que só se manifestam após certo tempo de uso), o prazo de 90 dias inicia-se no momento em que o defeito é detectado.

- **Responsabilidade Legal (CDC - Art. 18):**
  - Em caso de vício do produto, a Fornecedora deve sanar o defeito em no máximo **30 (trinta) dias**. Caso não o faça, o Consumidor (Instituição Contratante) a substituição do produto por outro da mesma espécie, em perfeitas condições de uso;

4.9.3. Os prazos de garantia serão contados a partir do recebimento definitivo do objeto, conforme previsto no art. 140, inciso II, alínea "b", da Lei nº 14.133, de 1º de abril de 2021.

4.10. Requisitos da Exigência de Prospecto e/ou Documentação Técnica

4.10.1. A exigência de apresentação de prospecto, catálogo técnico, documentação oficial ou material informativo constitui prática admissível em processos licitatórios relacionados à contratação de serviços e soluções tecnológicas, permitindo à Administração avaliar previamente a conformidade, compatibilidade e aderência das soluções ofertadas às necessidades institucionais da Defensoria Pública do Estado do Amapá.

4.10.2. A necessidade de apresentação de documentação técnica, catálogos, manuais oficiais ou prospectos será avaliada conforme a solução escolhida, visando assegurar o melhor atendimento às necessidades da Administração, condicionada à previsão expressa no Termo de Referência ou no edital do processo licitatório.

4.10.3. Para a solução de segurança de rede do tipo Next Generation Firewall (NGFW), a comprovação das funcionalidades e características técnicas poderá ocorrer mediante apresentação de documentação técnica oficial, catálogos, manuais do fabricante, datasheets, páginas oficiais do fabricante ou fornecedor, bem como demais materiais comprobatórios que demonstrem os recursos ofertados, incluindo funcionalidades de inspeção de tráfego, prevenção de intrusões, controle de aplicações, filtragem de conteúdo, VPN, alta disponibilidade, proteção contra ameaças avançadas e demais requisitos previstos no Termo de Referência.

4.10.4. Não será exigida prova de conceito (PoC), ambiente de teste ou apresentação de amostra física da solução, considerando a natureza dos equipamentos e serviços contratados, a ampla disponibilidade de documentação técnica oficial dos fabricantes e a necessidade de celeridade na tramitação do processo de contratação.

4.10.5. Todos os documentos, manuais, catálogos, prospectos e materiais técnicos deverão ser apresentados em língua portuguesa, sendo admitida tradução simples quando originalmente redigidos em outro idioma.

4.11. Da Garantia Contratual

4.11.1.Para a presente contratação, não será exigida garantia contratual, considerando as características e a natureza dos serviços a serem contratados, bem como a avaliação de que a exigência não se mostra necessária ou proporcional aos riscos envolvidos na execução do objeto

4.11.2. Independentemente da exigência ou não de garantia contratual, permanecerá integralmente sob responsabilidade da contratada o cumprimento das obrigações assumidas, incluindo disponibilidade da solução, prestação do suporte técnico, atendimento aos níveis de serviço estabelecidos e preservação da continuidade operacional da plataforma.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. ROTINA DE EXECUÇÃO DO OBJETO

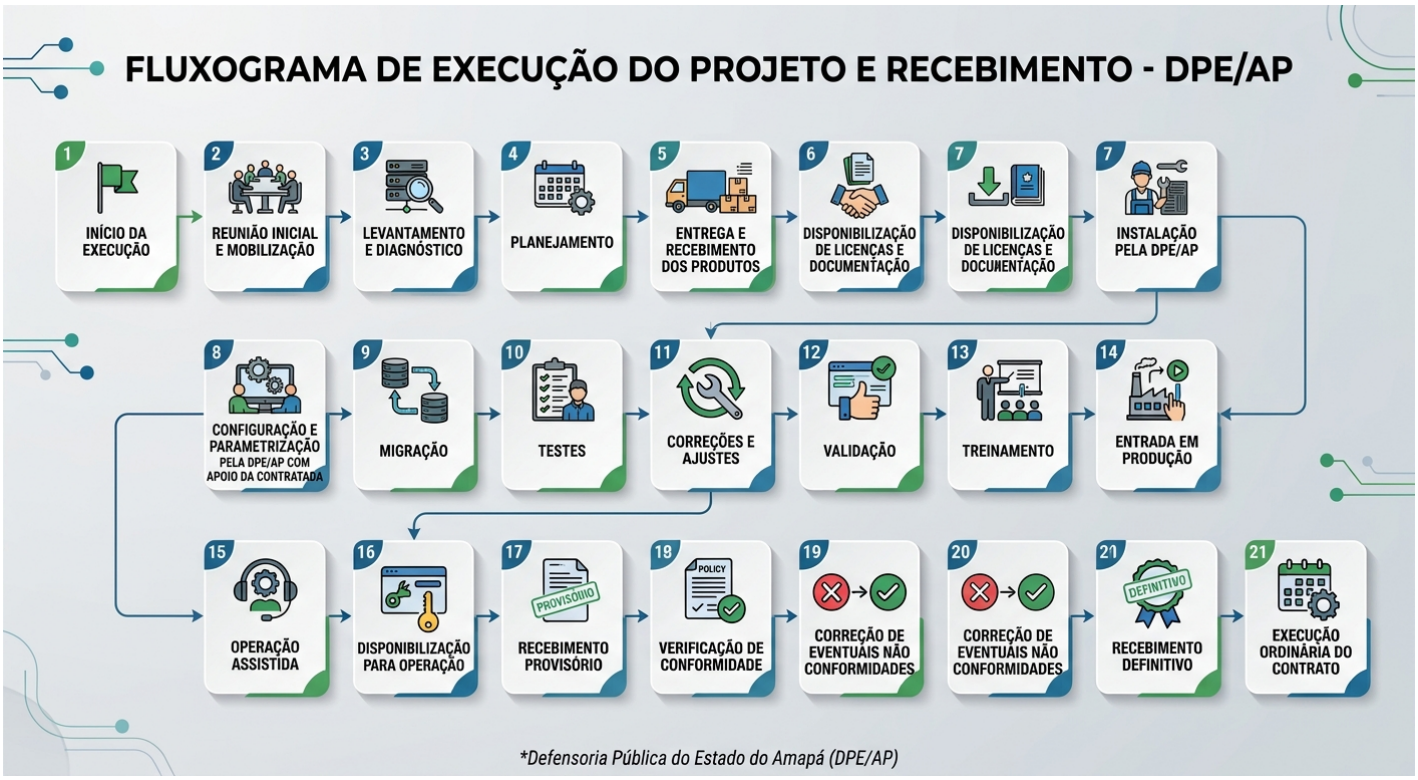
5.1.1. Fluxograma de Execução

5.1.1.1.A execução do objeto ocorrerá de forma planejada e coordenada, compreendendo o fornecimento e a disponibilização da solução de segurança de rede do tipo **Next Generation Firewall (NGFW)**, incluindo equipamentos, licenças, softwares, documentação técnica, instalação, configuração, migração, treinamento, suporte técnico, atualizações, manutenção e operação assistida, conforme estabelecido neste Termo de Referência.

5.1.1.2.A instalação, configuração e parametrização da solução serão realizadas pela equipe técnica da Defensoria Pública do Estado do Amapá, com apoio técnico especializado da contratada, a quem caberá fornecer a solução, documentação, orientações técnicas, suporte à implantação, migração, testes, validação, treinamento e operação assistida.

5.1.1.3.O fluxo de execução observará, preferencialmente, a seguinte sequência:

5.1.1.4. Início da Execução → Reunião Inicial e Mobilização → Levantamento e Diagnóstico → Planejamento → Entrega e Recebimento dos Produtos → Disponibilização de Licenças e Documentação → Instalação pela DPE/AP → Configuração e Parametrização pela DPE/AP com Apoio da Contratada → Migração → Testes → Correções e Ajustes → Validação → Treinamento → Entrada em Produção → Operação Assistida → Disponibilização para Operação → Recebimento Provisório → Verificação de Conformidade → Correção de Eventuais Não Conformidades → Recebimento Definitivo → Execução Ordinária do Contrato.



5.1.1.5.A sequência possui caráter operacional e orientativo, podendo determinadas atividades ocorrer de forma sucessiva, simultânea ou parcialmente sobreposta, conforme as características do ambiente e a estratégia de implantação adotada.

5.1.1.6.Não serão estabelecidos prazos individualizados entre as etapas de implantação, salvo quando expressamente previstos neste Termo de Referência ou no instrumento contratual. A inexistência desses prazos não afasta a responsabilidade das partes pelo cumprimento das atividades que lhes forem atribuídas.

5.1.1.7.Os procedimentos de **recebimento dos produtos, recebimento provisório e recebimento definitivo** possuem natureza própria e observarão os critérios, condições e prazos estabelecidos na seção específica deste Termo de Referência.

5.1.2. Disponibilização, Entrega e Recebimento dos Produtos

5.1.2.1. A contratada deverá disponibilizar e entregar, nos prazos estabelecidos neste Termo de Referência e no instrumento contratual, todos os equipamentos, licenças, softwares, subscrições, credenciais, códigos de ativação, documentação e demais elementos necessários à implantação e operação da solução.

5.1.2.2.O recebimento dos produtos será realizado pela Administração mediante conferência da quantidade, integridade, especificações e demais requisitos estabelecidos na contratação, sem prejuízo dos procedimentos de recebimento provisório e definitivo.

5.1.2.3. Eventuais divergências, avarias, ausência de componentes ou desconformidades deverão ser formalmente registradas, cabendo à contratada realizar as correções, substituições ou complementações necessárias, conforme as condições contratuais.

5.1.2.4.A entrega dos produtos não implica, por si só, o aceite definitivo do objeto, devendo

ser observadas as etapas de instalação, configuração, testes, validação e os procedimentos formais de recebimento previstos neste Termo de Referência.

5.1.2.5.A entrega deverá ser realizada nas dependências da Defensoria Pública do Estado do Amapá (Avenida Raimundo Alvares da Costa, nº 676, Bairro Centro, Macapá - AP, CEP: 68.900-074 - Anexo II), compreendendo transporte, descarregamento, conferência e demais procedimentos necessários ao recebimento definitivo, segunda a sexta-feira, das 07h30 às 16h30, no expediente da instituição, conforme a Portaria nº 412, de 8 de maio de 2024, e suas alterações, durante a execução do contrato.

5.1.2.2. A data de Entrega dos Produtos (prazo de até 30 dias)

5.1.2.2.1. Confirmada a demanda, a CONTRATADA deverá realizar a entrega dos produtos e/ou a execução dos serviços no prazo de até 30 (trinta) dias, contado na forma estabelecida neste Termo de Referência.

5.1.2.2.2.O prazo de entrega poderá ser prorrogado, por igual período, mediante solicitação formal e devidamente fundamentada da CONTRATADA, quando ocorrerem fatos supervenientes, imprevisíveis ou de consequências incalculáveis, alheios à sua vontade, que comprovadamente impeçam ou dificultem o cumprimento do prazo originalmente estabelecido.

5.1.2.2.3.A solicitação de prorrogação deverá ser apresentada pela CONTRATADA tão logo tenha conhecimento do fato que possa comprometer o cumprimento do prazo, acompanhada de documentação e elementos comprobatórios suficientes para demonstrar a ocorrência, a relação de causalidade com o atraso e a impossibilidade ou dificuldade de cumprimento do prazo original.

5.1.2.2.4.A concessão da prorrogação não será automática, ficando condicionada à análise e manifestação da CONTRATANTE, que avaliará a pertinência dos fatos alegados, a documentação apresentada e o impacto sobre o cumprimento das obrigações contratuais.

5.1.2.2.5.A prorrogação somente será admitida quando ficar comprovado que o evento não decorreu de ação ou omissão da CONTRATADA e que foram adotadas, por esta, todas as medidas razoavelmente disponíveis para evitar ou reduzir os efeitos do fato superveniente sobre o prazo de entrega.

5.1.2.2.6.Consideram-se, para fins deste dispositivo, sem prejuízo de outras situações devidamente comprovadas, eventos externos que possam afetar diretamente o fornecimento, tais como fatos da natureza, determinações de autoridades públicas, interrupções relevantes de transporte ou logística, indisponibilidade comprovada de componentes ou matérias-primas decorrente de eventos excepcionais, situações de força maior ou caso fortuito e outros acontecimentos alheios à esfera de controle da CONTRATADA.

5.1.2.2.7. A eventual concessão da prorrogação deverá ser formalizada pela CONTRATANTE, não implicando, por si só, alteração das demais obrigações, condições, preços ou quantitativos estabelecidos na contratação.

5.1.3. Implantação da Solução

5.1.3.1.A implantação compreenderá o levantamento e diagnóstico do ambiente, planejamento, instalação, configuração, parametrização, migração, testes, validação, treinamento, entrada em produção e operação assistida.

5.1.3.2.A contratada deverá fornecer apoio técnico especializado durante as atividades sob responsabilidade da equipe da Defensoria Pública, orientando quanto às boas práticas, requisitos técnicos, procedimentos de migração, configuração, testes e utilização da solução.

5.1.3.3.A equipe técnica da Defensoria Pública será responsável pela execução direta da instalação, configuração e parametrização, observadas as orientações técnicas do fabricante e o suporte disponibilizado pela contratada.

5.1.3.4.O planejamento deverá priorizar a continuidade dos serviços institucionais e a redução dos riscos de indisponibilidade durante a implantação e migração.

5.1.4. Testes, Validação e Entrada em Produção

5.1.4.1.Após a instalação, configuração e migração, serão realizados os testes técnicos e funcionais necessários à verificação da solução, incluindo, conforme aplicável, conectividade, roteamento, NAT, firewall, VPN, autenticação, segmentação, proteção contra ameaças, logs, monitoramento, alertas e integrações.

5.1.4.2.As inconsistências identificadas deverão ser corrigidas ou tratadas pela parte responsável, cabendo à contratada prestar o suporte necessário quando relacionadas à solução fornecida.

5.1.4.3.Concluídos os testes, a equipe técnica da Defensoria Pública realizará a validação da solução, verificando o funcionamento dos equipamentos, licenças, funcionalidades e integrações essenciais.

5.1.4.4.A entrada em produção ocorrerá após a conclusão satisfatória das atividades necessárias à disponibilização da solução, devendo ser planejada de forma a minimizar impactos e riscos de indisponibilidade.

5.1.5. Treinamento e Operação Assistida

5.1.5.1.A contratada deverá realizar treinamento para a equipe técnica indicada pela Defensoria Pública, contemplando a administração, configuração, monitoramento, análise de eventos e logs, políticas de segurança, atualizações, backup, restauração, contingência e demais funcionalidades necessárias à operação da solução.

5.1.5.2.Após a entrada em produção, a contratada prestará operação assistida pelo período estabelecido neste Termo de Referência, fornecendo suporte técnico especializado, orientação, auxílio na identificação e correção de inconsistências e apoio à estabilização do ambiente.

5.1.5.3.A operação assistida não transfere à contratada a responsabilidade pela administração ordinária da infraestrutura da Defensoria Pública, o suporte tem caracter preventivo durante a fase de implementação do novo sistema.

5.1.6. Documentação Final

5.1.6.1.Ao término da implantação, a contratada deverá disponibilizar a documentação técnica necessária à administração, operação, manutenção e suporte da solução, incluindo, conforme aplicável, arquitetura, equipamentos, licenças, versões, configurações, políticas de segurança, regras de firewall, VPNs, integrações, procedimentos de backup, restauração, atualização, contingência e demais informações relevantes.

5.1.7. Suporte, Atualizações e Manutenção

5.1.7.1.Durante a vigência contratual, a contratada deverá prestar suporte técnico especializado e disponibilizar as atualizações, correções, subscrições, mecanismos de segurança e demais recursos previstos na contratação.

5.1.7.2.O suporte compreenderá, conforme aplicável, diagnóstico e correção de falhas, orientação técnica, apoio à configuração, análise de eventos de segurança, atualização de software e firmware, atualização das bases de segurança, manutenção e substituição de equipamentos ou componentes, quando abrangidas pela contratação.

5.1.7.3.A prestação dos serviços observará os níveis de serviço, prazos de atendimento e demais condições estabelecidas neste Termo de Referência e no instrumento contratual.

5.1.8. Critérios de Recebimentos e Aceitação

5.1.8.1. Os critérios de recebimento e aceitação dos bens ou serviços observarão as disposições estabelecidas no item 7.3 deste Termo de Referência.

6. MODELO DE GESTÃO DO CONTRATO

6.1. MECANISMOS FORMAIS DE COMUNICAÇÃO

6.1.1. São definidos como mecanismos formais de comunicação, entre a CONTRATANTE e a CONTRATADA, os seguintes:

6.1.2. Ordem de Serviço;

6.1.3. Sistema de abertura de chamados;

6.1.4. E-mails.

6.2. OBRIGAÇÕES DA CONTRATADA

6.2.1. Cumprir fielmente o que estabelece este Termo de Referência, em especial no que se refere à implantação, operação e níveis de serviço;
6.2.2. Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais (LGPD). Para a habilitação, o licitante deverá apresentar Declaração indicando o encarregado responsável pela proteção de dados, nos termos do art. 41 da Lei Federal nº 13.709/18;
6.2.3. Executar o objeto conforme especificações deste Termo de Referência e de sua proposta;
6.2.4. Prestar os materiais dentro dos parâmetros e rotinas estabelecidos, fornecendo todo sempre que necessário suporte técnico, com a observância às recomendações aceitas pela boa técnica, normas e legislação;
6.2.5. Disponibilizar canais de atendimento para comunicação com a CONTRATANTE, observados os mecanismos formais de comunicação estabelecidos no item 6.1, especialmente o sistema de abertura de chamados, para registro, acompanhamento e tratamento das ocorrências relacionadas à execução do objeto.
6.2.6. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE por intermédio de preposto designado para acompanhamento do contrato nos seguintes prazos: em até 24 horas corridas, para as capitais estaduais e em até 72 horas, a contar de sua solicitação;
6.2.7. Promover a organização técnica e administrativa dos materiais, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado;
6.2.8. Indicar formalmente e por escrito, no prazo máximo de 24 horas úteis após a assinatura do contrato, junto à CONTRATANTE, um preposto idôneo, bem como seu superior imediato, com poderes de decisão para representar a CONTRATADA, principalmente no tocante à eficiência e agilidade da execução dos serviços objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato;
6.2.9. Reconhecer o Gestor do Contrato, bem como outros servidores que forem indicados pela CONTRATANTE, para realizar as solicitações relativas aos contratos a serem firmados, tais como manutenção, configuração, entre outras;
6.2.10. Apresentar Nota Fiscal/Fatura com a descrição dos materiais fornecidos nas condições deste Termo de Referência, como forma de dar início ao processo de pagamento pela CONTRATANTE;
6.2.11. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
6.2.12. Assumir as responsabilidades pelos encargos fiscais e comerciais resultantes da adjudicação da licitação oriunda deste Termo de Referência;
6.2.13. Assumir inteira responsabilidade técnica e operacional do objeto contratado, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por problemas de funcionamento do serviço;
6.2.14. Caso o problema de funcionamento das licenças detectado tenha a sua origem fora do escopo do objeto contratado, a CONTRATADA repassará para a CONTRATANTE as informações técnicas com a devida análise fundamentada que comprovem o fato, sem qualquer ônus para a CONTRATANTE;
6.2.15. Atender às solicitações os objetos contemplados no Termo de Referência, somente por Preposto designado;
6.2.16. Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE;
6.2.17. Responder por quaisquer interferências de estranhos nos acessos em serviço, bem como zelar pela integridade da comunicação;
6.2.18. Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;
6.2.19. Acatar as orientações da CONTRATANTE, sujeitando-se à mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo às reclamações formuladas;
6.2.20. Prestar esclarecimentos à CONTRATANTE sobre eventuais atos ou fatos noticiados que se refiram à CONTRATADA, independente de solicitação;
6.2.21. Comunicar à CONTRATANTE, por escrito, qualquer anormalidade dos serviços e prestar os esclarecimentos julgados necessários;
6.2.22. Manter, durante toda a execução do contrato, as mesmas condições da habilitação e qualificação exigidas na licitação, em compatibilidade com as obrigações assumidas;
6.2.23. Sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do art. 125 da Lei n° 14.133/21, quais sejam, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor atualizado do contrato;
6.2.24. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do Contrato, sem prévia autorização da CONTRATANTE;
6.2.25. Não fazer uso das informações prestadas pela CONTRATANTE para fins diversos do estrito e absoluto cumprimento do contrato em questão;

6.2.26. Garantir sigilo e inviolabilidade das conversações realizadas por meio do serviço desta contratação, respeitando as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações;
6.2.27. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços da CONTRATADA ensejará a responsabilidade criminal, na forma da lei, sem prejuízo de outras providências nas demais esferas;
6.2.28. Responder, integralmente, por perdas e danos que vier a causar à CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou de prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita; e
6.2.29. Cumprir outras obrigações que se apliquem, de acordo com o objeto da contratação.

6.3. OBRIGAÇÕES DA CONTRATANTE

6.3.1. Observar e fazer cumprir fielmente o que estabelece este Termo de Referência, em particular no que se refere aos níveis de serviço especificados;
6.3.2. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais;
6.3.3. Providenciar as assinaturas pela CONTRATADA no Termo de Compromisso de Manutenção de Sigilo e Respeito às Normas de Segurança e no Termo de Ciência da Declaração de Manutenção de Sigilo;
6.3.4. Prestar as informações e esclarecimentos relativos ao objeto desta contratação que venham a ser solicitado pelo preposto da CONTRATADA;
6.3.5. Dirimir as dúvidas que surgirem no curso do fornecimento dos materiais por intermédio do Gestor ou fiscal do Contrato.
6.3.6. Nomear Gestor e Fiscais para acompanhar e fiscalizar a execução do contrato;
6.3.7. Exercer o acompanhamento e a fiscalização dos materiais, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;
6.3.8. Encaminhar formalmente a demanda por meio de Ordem de Serviço, de acordo com os critérios estabelecidos neste Termo de Referência;
6.3.9. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;
6.3.10. Efetuar o pagamento dos serviços de acordo com as condições contratuais, no prazo e condições estabelecidas neste Termo de Referência, e no caso de cobrança indevida, glosar os valores considerados em desacordo com o contrato;
6.3.11. Após a notificação da glosa, a CONTRATADA terá prazo de 15 dias corridos para questionar os valores glosados, sob pena de ter-se por aceita a glosa;
6.3.12. Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;
6.3.13. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, assegurando à CONTRATADA a ampla defesa e o contraditório;
6.3.14.Liquidar o empenho e efetuar o pagamento à CONTRATADA para serviços regularmente prestados, dentro dos prazos preestabelecidos em contrato;
6.3.15. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com a prestação do serviço.

6.4. DA FISCALIZAÇÃO TÉCNICA, ADMINISTRATIVA E DO GESTOR DO CONTRATO

6.4.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, como prevê o art. 117, caput, da Lei Federal nº 14.133/2021.

6.4.2. Fiscalização técnica:

6.4.2.1.O fiscal acompanhará a execução, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração (Portaria 36/2024 - DPE/AP);
6.4.2.2.O fiscal anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à sua execução, com a descrição do que for necessário para a regularização das falhas ou dos defeitos observados (Lei Federal nº 14.133/2021, art. 117, § 1º e art. 20, II, da Portaria nº 36/2024 - DPE/AP);
6.4.2.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico emitirá notificações para a correção da execução do contrato, determinando prazo para a correção;
6.4.2.4. Informar o gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;
6.4.2.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas determinadas, o fiscal comunicará o fato imediatamente ao gestor do contrato;
6.4.2.6. Comunicar, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas a tempestiva renovação ou a prorrogação contratual;

6.4.3. Fiscalização administrativa:

6.4.3.1. O fiscal administrativo deverá verificar a manutenção das condições de habilitação da Contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitado quaisquer documentos comprobatórios pertinentes, caso necessário, como prevê o art. 21, incisos II e III da Portaria nº 36/2024 - DPE/AP.

6.4.3.2. Caso ocorra descumprimento das obrigações contratuais, o fiscal atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

6.4.4. Gestor do contrato:

6.4.4.1. O gestor do contrato coordena a atualização do processo de acompanhamento e fiscalização do contrato, contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborar relatórios com vistas a verificação da necessidade de adequações do contrato para fins de atendimento da finalidade administrativa. (art. 19, da Portaria nº 36/2024 - DPE/AP);

6.4.4.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato de toda as ocorrências relacionadas a execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior aqueles que ultrapassem a sua competência;

6.4.4.3. Acompanhará a manutenção das condições de habilitação da Contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

6.4.4.4. Emitirá o documento comprobatório da avaliação realizada pelos fiscais quanto ao cumprimento de obrigações assumidas pela Contratada, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar no cadastro de atesto de comunicações de obrigações (art. 19, VI, da Portaria nº 36/2024 - DPE/AP);

6.4.4.5. Tomará providências para a formalização do processo administrativo para fins de aplicação de sanções, a ser conduzida pela comissão que trata o art. 158 da Lei Federal nº 14.133/2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso (art. 19, VII da Portaria nº 36/2024 - DPE/AP).

6.4.5. Além do disposto acima, a fiscalização contratual obedecerá ao que prevê na Portaria nº 36/2024 - DPE/AP.

6.4.6. A fiscalização técnica e administrativa poderá ser exercida por um único servidor, conforme art. 23 da Portaria 36/2024 - DPE/AP.

6.4.7. O desempenho das atribuições do fiscal de contrato não exclui tampouco reduz a responsabilidade da Contratada, inclusive perante a terceiros, por qualquer irregularidade, ainda que resulte de imperfeições técnicas ou vícios redibitórios (art. 24 da Portaria nº 36/2024 - DPE/AP).

6.5. DAS SANÇÕES ADMINISTRATIVAS

6.5.1. O licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações:

6.5.1.1. a) Dar causa à inexecução parcial do contrato;

6.5.1.2. b) Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

6.5.1.3. c) Dar causa à inexecução total do contrato;

6.5.1.4. d) Deixar de entregar a documentação exigida para o certame;

6.5.1.5. e) Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

6.5.1.6. f) Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

6.5.1.7. g) Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

6.5.1.8. h) Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

6.5.1.9. i) Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

6.5.1.10. j) Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

6.5.1.11. k) Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

6.5.1.12. l) Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013

6.5.2. Serão aplicadas ao responsável pelas infrações administrativas previstas nesta Lei as seguintes sanções:

6.5.2.1. a) Advertência;

6.5.2.2. b) Multa;

6.5.2.3. c) Impedimento de licitar e contratar;

6.5.2.4. d) Declaração de inidoneidade para licitar ou contratar.

6.5.3. Na aplicação das sanções serão considerados:
6.5.3.1. a) A natureza e a gravidade da infração cometida;
6.5.3.2. b) As peculiaridades do caso concreto;
6.5.3.3. c) As circunstâncias agravantes ou atenuantes;
6.5.3.4. d) Os danos que dela provierem para a Administração Pública;
6.5.3.5. e) A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
6.5.4. Será aplicada advertência, de acordo com o artigo 156, inciso I, parágrafo §2º, infração administrativa previsto no inciso I do caput do art. 155, quando não se justificar a imposição de penalidade mais grave.
6.5.5. A aplicação de multa prevista no Art. 156, inciso II, de acordo com o parágrafo §3º, será calculada na forma do edital ou do contrato, não poderá ser inferior 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação direta e será aplicada ao responsável por qualquer das infrações administrativas previstas no art. 155 da Lei 14.133/2021.
6.5.6. A sanção de impedimento de licitar e contratar, será aplicada ao responsável pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do caput do artigo 155, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos.
6.5.7. A sanção declaração de inidoneidade para licitar ou contratar será aplicada ao responsável pelas infrações administrativas previstas nos incisos VIII, IX, X, XI e XII do caput do art. 155 da Lei 14.133/2021, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do caput do referido artigo que justifiquem a imposição de penalidade mais grave que a sanção referida no § 4º deste artigo, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.
6.5.8. A sanção estabelecida no inciso IV (declaração de inidoneidade para licitar ou contratar) do caput do artigo 156 será precedida de análise jurídica e observará as seguintes regras:
6.5.8.1. a) Quando aplicada por órgão do Poder Executivo, será de competência exclusiva de ministro de Estado, de secretário estadual ou de secretário municipal e, quando aplicada por autarquia ou fundação, será de competência exclusiva da autoridade máxima da entidade;
6.5.8.2. b) Quando aplicada por órgãos dos Poderes Legislativo e Judiciário, pelo Ministério Público e pela Defensoria Pública no desempenho da função administrativa, será de competência exclusiva de autoridade de nível hierárquico equivalente às autoridades referidas no inciso I deste parágrafo, na forma de regulamento.
6.5.9. As sanções previstas nos incisos I, (advertência) III (impedimento de licitar e contratar) e IV (declaração de inidoneidade para licitar ou contratar) do caput do artigo 156, poderão ser aplicadas cumulativamente com a prevista no inciso II (multa) do caput deste artigo.
6.5.10. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.
6.5.11. A aplicação das sanções previstas no caput do artigo 156 não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.
6.5.12. O atraso injustificado na execução do contrato sujeitará o contratado à multa de mora, na forma prevista em edital ou em contrato.
6.5.13. A aplicação de multa de mora não impedirá que a Administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções previstas nesta Lei.

7. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

7.1. A medição se dará pela entrega integral dos serviços e acesso as assinaturas as licenças conforme contrato, instrumento equivalente ou ordem de serviço considerado o grau de conformidade com normas técnicas pertinentes.
7.2. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada :
7.2.1. não produzir os resultados acordados,
7.2.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou
7.2.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utiliza-los com qualidade ou quantidade inferior à demandada.

7.3. Recebimento do objeto

7.3.1. Os equipamentos e serviços complementarem serão recebidos provisoriamente, no prazo de 05

(cinco) dias, pelos fiscais técnicos, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico, além da verificação de suas conformidades com as especificações constantes no Termo de Referência, planilhas e proposta.

7.3.2.O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico**.**

7.3.3. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

7.3.4.O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo

7.3.5. A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar os serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.3.6. A fiscalização não efetuará o ateste dos objetos até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório**.**

7.3.7. Os objetos poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos/corrigidos no prazo de 3 (três) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.3.8. O prazo para o Recebimento Definitivo das licenças e códigos de acesso, iniciar-se-á a partir da data de atestação do início da efetiva operação e funcionamento pleno dos serviços da Contratante. As licenças e acesso aos serviços serão recebidos definitivamente no prazo de até 10 (dez) dias úteis, a contar do marco inicial acima, sendo o procedimento conduzido e formalizado pelo Gestor do Contrato, mediante verificação da qualidade, quantidade e consequente aceitação por meio de Termo de Recebimento Definitivo detalhado

7.3.9. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.3.10. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.3.11. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

7.3.12. Emitir Termo Detalhado para efeito de recebimento definitivo dos materiais fornecidos, com base nos relatórios e documentações apresentadas; e

7.3.13. Comunicar à empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

7.3.14. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

7.3.15. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.3.16. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.3.17. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

7.4. Liquidação

7.4.1. Recebida a nota fiscal ou documento de cobrança equivalente, ocorrerá no prazo de 10 (dez) dias úteis para fins de liquidação da despesa.

7.4.1.1. O prazo de que trata o item anterior poderá ser excepcionalmente prorrogado, justificadamente, por igual período, quando houver necessidade de diligências para aferição ao atendimento das exigências contratuais, conforme art. 7º, § 3º, da Portaria nº 47/2024 - DPE/AP.

7.4.2. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou documento equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

7.4.2.1. o prazo de validade;

7.4.2.2. a data da emissão;
7.4.2.3. os dados do contrato e do órgão requisitante;
7.4.2.4. o período respectivo de execução do contrato;
7.4.2.5. o valor a pagar; e
7.4.2.6. eventual destaque do valor de retenções tributárias cabíveis.
7.4.3. Havendo erro na nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestado até que o contratada providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus para a DPE/AP.
7.4.4. A nota fiscal ou documento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta online ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais.
7.4.5.A Administração deverá realizar consulta ao SICAF para:

a) verificar a manutenção das condições de habilitação exigidas;
b) identificar possível razão que impeça a participação em licitação/contratação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

7.4.6. Constatando-se junto ao SICAF, a situação da irregularidade do contratado, será providenciada sua notificação, por escrito, para que no prazo de 05 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez por igual período, a critério da DPE/AP.
7.4.7.Não havendo regularização ou sendo a defesa considerada improcedente, a DPE/AP 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 adicionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
7.4.8. Persistindo a irregularidade, a DPE/AP deverá adotar medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.
7.4.9. 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.

7.5. Prazo de pagamento

7.5.1. O pagamento será efetuado no prazo máximo de 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme item 7.4 e seus subitens, nos termos do inciso II, art. 7º, da Portaria nº 47/2024 - DPE/AP.
7.5.2. No caso de atraso pela DPE/AP, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice de Custo da Tecnologia da Informação (ICTI) - de correção monetária.

7.6. Forma de pagamento

7.6.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.
7.6.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
7.6.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
7.6.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.
7.6.5. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá 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. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

8.1. Não se aplica por se tratar de Sistema de Registro de Preços.

9. DA VIGÊNCIA DO CONTRATO E DO ÍNDICE DE REAJUSTE DE PREÇO

9.1. Considerando que a presente contratação será realizada por meio de Pregão Eletrônico e tem por objeto o fornecimento de Solução de Proteção de Perímetro do tipo NGFW (Next Generation Firewall), contemplando equipamentos, licenças inerentes ao funcionamento da solução, implantação, garantia do fabricante, suporte

técnico especializado, repasse de conhecimento, solução de gestão centralizada, solução de gestão de logs e relatórios e banco de serviços técnicos especializados, mostra-se necessária a formalização de instrumento contratual para assegurar a adequada execução do objeto, a definição das obrigações das partes e a preservação da segurança jurídica da contratação.

9.2.A contratação possui natureza de **fornecimento e prestação de serviço associado**, nos termos do art. 6º, inciso XXXIV, da Lei Federal nº 14.133/2021, uma vez que compreende não apenas o fornecimento dos equipamentos, licenças e softwares que integram a solução NGFW, mas também a prestação de serviços associados necessários à sua adequada implantação, operação, sustentação e manutenção, incluindo instalação, configuração, migração de ambiente, treinamento, operação assistida, garantia, suporte técnico especializado, atualizações, manutenção corretiva e evolutiva e demais serviços previstos neste Termo de Referência.

9.3.A caracterização como fornecimento e prestação de serviço associado decorre da necessidade de assegurar a continuidade e a efetividade da solução de segurança durante todo o período de sua utilização, considerando que a finalidade da contratação não se esgota com a entrega e instalação dos equipamentos. Os serviços associados constituem parte integrante da solução contratada e são necessários para garantir seu funcionamento adequado, a atualização dos mecanismos de proteção, a correção de falhas, o suporte especializado e a manutenção das condições de segurança da infraestrutura tecnológica da Instituição.

9.4. Nos termos do art. 95 da Lei Federal nº 14.133/2021, a formalização por instrumento contratual mostra-se necessária em razão da natureza e da complexidade do objeto, que envolve obrigações futuras relacionadas ao fornecimento da solução e à prestação dos serviços associados, incluindo implantação, suporte técnico especializado, garantia, atualizações, manutenção, operação assistida e demais obrigações que permanecem durante a execução contratual.

9.5.A vigência dos contratos decorrentes da presente contratação será estabelecida de acordo com as características e necessidades da solução, podendo alcançar o período de 60 (sessenta) meses, observadas as disposições do art. 113 da Lei Federal nº 14.133/2021, aplicáveis aos contratos de fornecimento e prestação de serviço associado, bem como as demais disposições legais pertinentes.

9.6.O prazo de 60 (sessenta) meses justifica-se pela necessidade de assegurar a continuidade da proteção da infraestrutura de rede da Instituição, bem como a disponibilidade dos serviços de suporte técnico, atualização, manutenção, garantia e demais serviços associados à solução NGFW, permitindo a adequada sustentação tecnológica do ambiente durante seu ciclo de utilização e evitando descontinuidades que possam comprometer a segurança da informação e a disponibilidade dos serviços institucionais.

9.7.O instrumento contratual deverá disciplinar, dentre outros aspectos, as condições de entrega e recebimento dos equipamentos, os procedimentos de implantação e migração, os níveis mínimos de serviço (SLA), os prazos para atendimento e solução de chamados, as condições de garantia e suporte técnico, os procedimentos de atualização e manutenção da solução, os critérios para utilização do banco de serviços técnicos especializados, as responsabilidades relativas ao repasse de conhecimento e treinamento, os mecanismos de fiscalização e gestão contratual e os procedimentos para aplicação de sanções administrativas.

9.8. Embora o art. 95 da Lei Federal nº 14.133/2021 admita, em situações específicas, a substituição do instrumento contratual por nota de empenho, autorização de compra ou outro instrumento hábil, tal faculdade não se mostra adequada à presente contratação, diante da complexidade da solução e da existência de obrigações de execução continuada e de serviços associados, cuja disciplina exige a definição pormenorizada das responsabilidades das partes, dos níveis de serviço, dos mecanismos de fiscalização, dos procedimentos de manutenção e suporte e das demais condições necessárias à adequada execução do objeto.

9.9. Assim, considerando a natureza estratégica e crítica da solução NGFW para a proteção dos ativos de informação, a continuidade dos serviços institucionais, o controle dos acessos à rede e a prevenção, detecção e tratamento de ameaças cibernéticas, a adoção do regime de fornecimento e prestação de serviço associado mostra-se compatível com as necessidades da Administração, permitindo a contratação de uma solução integrada e sua adequada sustentação durante o período de utilização, em conformidade com a legislação aplicável.

9.10. Reajuste de Preços: O índice a ser utilizado para o reajuste anual dos preços contratuais, conforme a periodicidade e as regras estabelecidas neste instrumento e na legislação aplicável, deverá ser o Índice de Custo da Tecnologia da Informação (ICTI), calculado e divulgado oficialmente pelo Ipea (Instituto de Pesquisa Econômica Aplicada).

10. DEFINIÇÃO DE CRITÉRIOS TÉCNICOS PARA JULGAMENTO DA PROPOSTA

10.1. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1.1. Forma de seleção e critério de julgamento da proposta

10.1.1.1. O fornecedor será selecionado por meio da realização de procedimento de licitação, na modalidade Pregão, sob a forma Eletrônica, com adoção do critério de julgamento pelo **menor preço global do grupo** pelo procedimento auxiliar Sistema de Registro de Preços.

10.1.1.2. O critério de menor preço considerará o menor dispêndio para a Defensoria Pública, atendidos os parâmetros mínimos de qualidade e as demais exigências definidas neste Termo de Referência e no Edital de Licitação, nos termos do art. 6º, da Portaria nº 40/2024 - DPE/AP.

10.1.1.3. Os custos indiretos, relacionados às despesas de manutenção, utilização, reposição, depreciação e impacto ambiental, entre outros fatores vinculados ao seu ciclo de vida, poderão ser considerados para a definição do menor dispêndio, sempre que objetivamente mensuráveis, de acordo com o § 1º do artigo 34 da Lei Federal nº 14.133/2021, bem como com o § 1º do artigo 6º da Portaria nº 40/2024 - DPE/AP.

10.1.2. Exigências de habilitação

10.1.2.1. Para fins de habilitação, o licitante deverá comprovar os seguintes requisitos:

10.1.2.1.1. Habilitação jurídica

10.1.2.1.1.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

10.1.2.1.1.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.1.2.1.1.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

10.1.2.1.1.4. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

10.1.2.1.1.5. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

10.1.2.1.1.6. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.1.2.1.1.7. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

10.1.2.1.1.8. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

10.1.2.1.2. Habilitação fiscal, social e trabalhista

10.1.2.1.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

10.1.2.1.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

10.1.2.1.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

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

10.1.2.1.2.5. Prova de inscrição no cadastro de contribuintes Estadual ou Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.1.2.1.2.6. Prova de regularidade com a Fazenda Estadual ou Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

10.1.2.1.2.7. Cumprimento do disposto no inciso XXXIII do art. 7º da CF/88 (proibição de trabalho

noturno, perigoso ou insalubre a menores de 18 anos e de qualquer trabalho a menores de 16, salvo na condição de aprendiz, a partir de 14 anos).

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

10.1.2.1.2.9. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

10.1.2.1.3. Qualificação Econômico-Financeira

10.1.2.1.3.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea "c", da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

10.1.2.1.3.2. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

10.1.2.1.3.3. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

10.1.2.1.3.3.1. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos pelas seguintes fórmulas:

10.1.2.1.3.3.2. Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo)/(Passivo Circulante + Passivo Não Circulante);

10.1.2.1.3.3.3. Solvência Geral (SG)= (Ativo Total)/(Passivo Circulante +Passivo não Circulante); e

10.1.2.1.3.3.4. Liquidez Corrente (LC) = (Ativo Circulante)/(Passivo Circulante).

10.1.2.1.3.4. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação capital mínimo de 1% (um por cento) do valor total estimado da contratação.

10.1.2.1.3.5. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

10.1.2.1.3.6. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º).

10.1.2.1.4. Qualificação Técnica

10.1.2.1.4.1. Comprovação de aptidão para o fornecimento dos serviços com a complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

10.1.2.1.4.2. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

10.1.2.1.4.3. O atestado de capacidade técnica deverá comprovar o fornecimento na quantidade mínima de 10% (dez por cento) do total registrado para o item correspondente ao atestado.

10.1.2.1.4.4. O atestado deverá ser datado e assinado e deverá conter informações que permitam a identificação correta da contratante e do fornecedor, tais como:

- Nome, CNPJ e endereço do emitente;
- Nome, CNPJ e endereço da empresa que forneceu o bem ao emitente;
- Nome, cargo ou função do signatário emitente do atestado;

10.1.2.1.4.5. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

10.1.2.1.4.6. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

10.1.2.1.4.7. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Defensoria Pública do Estado do Amapá

- DPE/AP, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.,

10.1.2.1.4.8. A licitante deverá comprovar a disponibilidade de, no mínimo, 1 (um) profissional com certificação **PMP (Project Management Professional)**, emitida pelo **PMI (Project Management Institute)**, para atuação nas atividades de gerenciamento e acompanhamento do projeto durante a implantação da solução.

10.1.2.1.4.8.1. Para fins de habilitação, a licitante poderá comprovar a disponibilidade do profissional certificado PMP mediante:

a) comprovação do vínculo funcional ou contratual com o profissional, por meio de documento hábil; **ou**

b) apresentação de **Termo de Compromisso ou Declaração de Disponibilidade**, firmado pelo profissional ou pela licitante, conforme o caso, no qual seja assegurada formalmente a disponibilização de profissional que possua a certificação PMP para atuação na execução do objeto, caso a licitante venha a ser declarada vencedora.

10.1.2.1.4.8.2. Na hipótese de a licitante optar, na fase de habilitação, pela apresentação de Termo de Compromisso ou Declaração de Disponibilidade, a comprovação do efetivo vínculo com o profissional certificado PMP deverá ser apresentada pela licitante vencedora **como condição para a assinatura do contrato**, no prazo estabelecido para sua convocação e formalização da contratação.

10.1.2.1.4.8.3. Para fins do subitem anterior, serão admitidos, dentre outros instrumentos juridicamente hábeis, a **Carteira de Trabalho e Previdência Social – CTPS, contrato de prestação de serviços, contrato de trabalho ou outro documento apto a comprovar o vínculo ou a relação jurídica entre a CONTRATADA e o profissional indicado**.

10.1.2.1.4.8.4. A não apresentação, pela licitante vencedora que tenha optado pela Declaração de Disponibilidade ou Termo de Compromisso, da comprovação do efetivo vínculo com o profissional certificado PMP no prazo estabelecido para a assinatura do contrato implicará a **decadência do direito à contratação**, sem prejuízo da aplicação das sanções administrativas cabíveis, observado o disposto no art. 90, § 5º, c/c art. 155, inciso VI, da Lei Federal nº 14.133/2021.

10.1.2.1.4.8.5. Na ocorrência da situação prevista no subitem anterior, a Administração poderá adotar as providências previstas na legislação aplicável, inclusive quanto à **convocação das licitantes remanescentes, observada a ordem de classificação**, para os fins de contratação.

10.1.2.1.4.8.6. O profissional indicado deverá efetivamente participar das atividades relacionadas ao gerenciamento e acompanhamento do projeto durante a fase de implantação da solução, não sendo admitida sua substituição por profissional sem a certificação exigida, salvo mediante autorização prévia da CONTRATANTE e desde que o substituto possua qualificação técnica equivalente ou superior à exigida neste Termo de Referência.

10.1.2.1.4.8.7. A exigência da certificação PMP justifica-se pela necessidade de assegurar que a execução das atividades de implantação, gerenciamento, acompanhamento, controle de etapas, identificação de riscos e coordenação das atividades relacionadas à solução seja conduzida por profissional com qualificação reconhecida em gerenciamento de projetos.

11. DA SUBCONTRATAÇÃO

11.1. Não será admitida a subcontratação do objeto.

11.2. A vedação à subcontratação justifica-se pela criticidade dos serviços, especialmente quanto à segurança da informação, à confidencialidade e à proteção dos dados institucionais.

11.3.A medida visa assegurar o controle direto sobre o tráfego de dados, os acessos e os mecanismos de segurança, reduzindo riscos de exposição e garantindo maior rastreabilidade e confiabilidade na execução dos serviços.

11.4. É admissível a fusão, cisão ou incorporação da Contratada com/por outra pessoa jurídica, desde que:

a)sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; b)sejam mantidas as demais cláusulas e condições do contrato; c) não haja prejuízo à execução do objeto pactuado; d) haja a anuência expressa da Contratante à continuidade do contrato;

12. DA JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

12.1. A presente contratação será realizada por grupo de itens, sendo o Grupo 01 composto por 08 (oito) itens,

cujo julgamento ocorrerá pelo critério de menor preço global do grupo. O agrupamento mostra-se tecnicamente necessário em razão da natureza integrada da solução de segurança de perímetro baseada em tecnologia Next Generation Firewall (NGFW), uma vez que os equipamentos, licenças, softwares, serviços de suporte, gerenciamento centralizado, atualizações de segurança e demais componentes possuem relação de complementaridade e interdependência, devendo ser fornecidos, implantados e suportados por um único fornecedor, a fim de assegurar a plena compatibilidade da solução, a centralização da responsabilidade contratual e a adequada execução do objeto.

12.2. Embora a contratação contemple diversos itens, estes constituem partes integrantes de uma única solução tecnológica, cuja efetividade depende da compatibilidade, integração e funcionamento conjunto de todos os seus componentes. A eventual divisão da contratação entre diferentes fornecedores poderia comprometer a interoperabilidade da solução, dificultar a gestão centralizada do ambiente de segurança e gerar riscos relacionados à integração, desempenho e suporte técnico.

12.3. A solução NGFW contempla funcionalidades avançadas de segurança, tais como inspeção profunda de pacotes (Deep Packet Inspection – DPI), prevenção e detecção de intrusões (IPS/IDS), controle de aplicações, inspeção de tráfego criptografado, inteligência contra ameaças, redes privadas virtuais (VPN), monitoramento e geração de relatórios. Tais funcionalidades são desenvolvidas para operar de forma integrada dentro de um mesmo ecossistema tecnológico, sendo recomendável que todos os componentes sejam fornecidos e suportados por um único fornecedor responsável pela solução.

12.4. A fragmentação da contratação poderia ocasionar incompatibilidades técnicas entre equipamentos, licenças e módulos de segurança, além de dificultar a aplicação uniforme de atualizações, correções de vulnerabilidades e políticas de segurança. Adicionalmente, a existência de múltiplos fornecedores aumentaria a complexidade da gestão contratual e poderia gerar conflitos de responsabilidade em situações de falhas, indisponibilidades ou incidentes de segurança.

12.5. A contratação por grupo proporciona maior eficiência na implantação da solução, na migração do ambiente atualmente existente, na transferência de conhecimento, na operação assistida e no suporte técnico especializado, assegurando a uniformidade das configurações e a padronização tecnológica da infraestrutura de segurança institucional.

12.6. Sob o aspecto econômico, a contratação conjunta dos componentes da solução possibilita ganhos de escala, otimização dos custos de implementação, simplificação da gestão contratual e maior previsibilidade quanto aos níveis de serviço, suporte e garantia oferecidos durante toda a vigência contratual.

12.7. Dessa forma, a adoção do critério de julgamento pelo menor preço global do Grupo 01 mostra-se tecnicamente justificada e alinhada aos princípios da eficiência, economicidade, planejamento, segurança da informação e continuidade do serviço público, garantindo o atendimento integral das necessidades institucionais relacionadas à proteção dos ativos tecnológicos, dos dados e dos sistemas da Defensoria Pública do Estado do Amapá.

13. DO CUSTO ESTIMADO

13.1. O valor estimado para a presente contratação, na modalidade de Pregão Eletrônico, pelo Sistema de Registro de Preços é de **13.818.774,76 (treze milhões, oitocentos e dezoito mil setecentos e setenta e quatro reais e setenta e seis centavos).**

13.1. Em observância ao art. 7º da Portaria nº 38/2024 - DPE/AP e considerando o baixo grau de complexidade do objeto e o seu caráter comum, bem como os documentos que compõem a instrução do processo licitatório, verifica-se que as informações contidas neste Termo de Referência não necessitam de classificação da informação, nos termos da Lei nº 12.527/2011, e estarão disponíveis para consulta quando da publicação do Edital.

Macapá-AP, data da assinatura eletrônica.

(Assinatura eletronicamente)
ROGÉRIO LEITE MORESCO
Assessor Técnico Nível III
Coordenadoria de Licitações, Contratos e Convênios

Portaria nº 1103, de 03 de Outubro de 2023

APÊNDICE I - ANEXO I - ESPECIFICAÇÃO TÉCNICA DOS EQUIPAMENTOS

CARACTERÍSTICAS GERAIS PARA SOLUÇÃO DE PROTEÇÃO DE BORDA COM NGFW (NEXT GENERATION FIREWALL), ITENS 01, 02, 03, 04 e 05 (TIPOS 01 a 05).

- 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.
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
- Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderá estar listado no site do fabricante em listas de end-of-life e end-of-sale.
- 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.
- As funcionalidades de proteção de rede que compõem a solução de segurança podem funcionar em múltiplos appliances, desde que atendam a todos os requisitos desta especificação.
- Deverá possuir e estar licenciada pelo período de 60 (sessenta) meses com as seguintes funcionalidades: Firewall, Traffic Shaping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS) e VPN.
- Os appliances deverão ser instalados e configurados e/ou deverá ser realizada a migração dos dispositivos atuais da CONTRATANTE para as novas tecnologias, de forma presencial, por técnico certificado pelo fabricante, nas dependências da CONTRATANTE. Somente para os appliances da Capital; para as demais localidades, a instalação será de responsabilidade da CONTRATANTE, com suporte remoto da CONTRATADA.

FUNCIONALIDADES DE REDE E FIREWALL

- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- Os dispositivos de proteção de rede devem possuir suporte a VLANs;
- Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
- Os dispositivos de proteção de rede devem suportar subinterfaces Ethernet lógicas;
- 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, NAT66, NAT46 e PAT;
- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- Deverá suportar sFlow ou NetFlow;
- Deve possuir suporte à criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
- Deve suportar o protocolo padrão da indústria VXLAN;
- Deve implementar o protocolo ECMP;
- Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- Deve enviar logs para sistemas de monitoração externos;
- Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- Deve possuir mecanismos de proteção anti-spoofing;
- Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
- Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- Deve suportar OSPF graceful restart;
- Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

- Deve suportar Modo Camada 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- Deve suportar Modo Camada 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- Deve suportar configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- A configuração em alta disponibilidade deve sincronizar sessões, configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QoS e objetos de rede, associações de segurança das VPNs e tabelas FIB;
- 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;
- O modo de Alta Disponibilidade (HA) deve possibilitar monitoração de falha de link;
- A solução deve suportar integração nativa com Let's Encrypt, para obtenção automática de certificados válidos;
- A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXi, Cisco ACI e Kubernetes;
- Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls, suportando, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança predefinidos;
- Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- Deverá suportar controle por zonas de segurança;
- Deverá suportar controles de políticas por porta e protocolo;
- Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- Deverá suportar Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização;
- Deve suportar controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- Deve suportar controle de políticas por código de país (por exemplo: BR, US, UK, RU);
- Deve suportar controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
- Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
- Deve permitir o bloqueio de arquivos por sua extensão e possibilitar a correta identificação do arquivo por seu tipo, mesmo quando sua extensão for renomeada;
- Deve suportar objetos e regras IPv6;
- Deve suportar objetos e regras multicast;
- Deve suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários predefinidos automaticamente.

FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

- Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- Deve ser possível a liberação e o bloqueio somente de aplicações, sem a necessidade de liberação de portas e protocolos;
- Deve reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, atualização de software, protocolos de rede, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail;
- Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
- Deve 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 e google-docs;
- Deve inspecionar o payload do pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo;

- Deve 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;
- Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 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 específicas dentro de uma aplicação;
- Deve identificar o uso de táticas evasivas via comunicações criptografadas;
- Deve atualizar automaticamente a base de assinaturas de aplicações;
- 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;
- Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente à possibilidade de habilitar controle de aplicações em algumas regras;
- Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- Deve 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;
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- Deve alertar o usuário quando uma aplicação for bloqueada;
- Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (Bittorrent, Emule etc.), possuindo granularidade de controle e políticas para os mesmos;
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat etc.), possuindo granularidade de controle e políticas para os mesmos;
- Deve possibilitar a diferenciação e o controle de partes das aplicações, como, por exemplo, permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;
- Deve possibilitar a diferenciação de aplicações proxy (Psiphon, Freegate etc.), possuindo granularidade de controle e políticas para as mesmas;
- Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações, tais como: tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol etc.);
- Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações, tais como: nível de risco da aplicação, tecnologia, fabricante e popularidade;
- Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações, tais como: categoria da aplicação;
- Deve permitir forçar o uso de portas específicas para determinadas aplicações.

FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

- 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;
- Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- Deve sincronizar as assinaturas de IPS, Antivírus e Anti-Spyware quando implementado em alta disponibilidade;
- Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar o IP do atacante por um intervalo de tempo;
- As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- Deve ser possível definir exceções por IP de origem ou de destino nas regras ou assinatura por assinatura;
- 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;

- Deve permitir o bloqueio de vulnerabilidades;
- Deve permitir o bloqueio de exploits conhecidos;
- Deve incluir proteção contra ataques de negação de serviço;
- Deve ser imune e capaz de impedir ataques básicos como: SYN Flood, ICMP Flood, UDP Flood, entre outros;
- Deve detectar e bloquear a origem de port scans;
- Deve bloquear ataques efetuados por worms conhecidos;
- Deve possuir assinaturas específicas para mitigação de ataques DoS e DDoS;
- Deve possuir assinaturas para bloqueio de ataques de buffer overflow;
- Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- Deve permitir o uso de operadores de negação na criação de assinaturas customizadas de IPS ou Anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- Deve permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- Deve identificar e bloquear comunicação com botnets;
- Deve registrar na console de monitoração as seguintes informações sobre ameaças identificadas: nome da assinatura ou do ataque, aplicação, usuário, origem e destino da comunicação, além da ação tomada pelo dispositivo;
- Os eventos devem identificar o país de origem da ameaça;
- Deve incluir proteção contra vírus em conteúdo HTML e JavaScript, software espião (spyware) e worms;
- Deve possuir proteção contra downloads involuntários, utilizando HTTP, de arquivos executáveis e maliciosos;
- Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseadas nas políticas do firewall, considerando usuários, grupos de usuários, origem, destino, zonas de segurança e demais critérios, ou seja, cada política de firewall poderá possuir uma configuração distinta de IPS;
- A solução deve ter capacidade de enviar artefatos suspeitos para execução em ambiente controlado na nuvem do fabricante;
- Deve suportar a captura de pacotes (PCAP) por assinatura de IPS ou por controle de aplicação;
- Deve permitir que, na captura de pacotes por assinaturas de IPS, seja definido o número de pacotes a serem capturados ou possibilitar a captura do pacote que originou o alerta, bem como seu contexto, facilitando a análise forense e a identificação de falsos positivos.

FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

- Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- 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;
- 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;
- Deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação e validação das URLs;
- Deve possuir pelo menos 70 (setenta) categorias de URLs;
- Deve possuir a função de exclusão de URLs do bloqueio;
- Deve permitir a customização da página de bloqueio;
- Deve permitir a restrição de acesso a canais específicos do YouTube, possibilitando configurar uma lista de canais liberados ou uma lista de canais bloqueados;

- 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;
- Deve possuir a função de proteção à resolução de endereços via DNS, identificando requisições de resolução de nomes para domínios maliciosos e servidores de Comando e Controle (C&C) de botnets conhecidas;
- Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizada.

FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

- 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;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários;
- Deve possuir integração e suporte ao Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários, suportando Single Sign-On (SSO). Essa funcionalidade não deve possuir limites licenciados de usuários;
- Deve possuir integração com RADIUS para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários;
- Deve possuir integração com LDAP para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários;
- Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída para a Internet, de modo que, antes de iniciar a navegação, seja apresentado um portal de autenticação residente no firewall (Captive Portal);
- Deve possuir suporte à 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 nesses serviços;
- Deve suportar o envio e recebimento de credenciais via RADIUS;
- Deve implementar a criação de grupos customizados de usuários no firewall, baseados em atributos do LDAP/AD.

FUNCIONALIDADE DE FILTRO DE DADOS

- Deve permitir identificar e, opcionalmente, prevenir a transferência de vários tipos de arquivos (MS Office, PDF etc.) identificados sobre aplicações (HTTP, FTP, SMTP);
- Deve suportar a identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- Deve suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- Deve permitir identificar e, opcionalmente, prevenir a transferência de informações sensíveis, incluindo, mas não limitado a números de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

FUNCIONALIDADE DE GEOLOCALIZAÇÃO

- Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado país ou países seja bloqueado;
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

FUNCIONALIDADE DE VPN

- Deve suportar VPN Site-to-Site e Client-to-Site;
- Deve suportar IPSec VPN;

- A VPN IPSec deve suportar 3DES;
- A VPN IPSec deve suportar autenticação MD5 e SHA-1;
- A VPN IPSec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- A VPN IPSec deve suportar Internet Key Exchange (IKEv1 e IKEv2);
- A VPN IPSec deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- A VPN IPSec deve suportar autenticação via certificado IKE PKI;
- Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet e SonicWall;
- Deve suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
- Deve permitir habilitar e desabilitar túneis de VPN IPSec a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 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;
- Deve permitir atribuição de DNS aos clientes remotos de VPN;
- Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Spyware e filtro de URL para o tráfego dos clientes remotos conectados na VPN;
- Deve suportar autenticação via AD/LDAP, Secure ID, certificado e base de usuários local;
- Deve suportar leitura e verificação de CRL (Certificate Revocation List);
- Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis VPN;
- Deve permitir que a conexão com a VPN seja estabelecida após autenticação do usuário na estação;
- Deve permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
- Deverá manter uma conexão segura com o portal durante a sessão;
- O agente de VPN Client-to-Site deve ser compatível com, pelo menos:
- Windows 10 e superior;
- Linux Ubuntu 22.04 e superior;
- Linux Red Hat 9;
- Linux CentOS 9;
- macOS 13 e superior.

FUNCIONALIDADE DE QoS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

- Com a finalidade de controlar aplicações e tráfegos cujo consumo possa ser excessivo, a solução deverá possuir a capacidade de controlá-los por políticas de largura de banda;
- Deve suportar a criação de políticas de QoS e Traffic Shaping para:
- Endereço de origem;
- Endereço de destino;
- Usuário e grupo;
- Aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- Porta;
- O QoS deve possibilitar a definição de tráfego com banda garantida;
- O QoS deve possibilitar a definição de tráfego com banda máxima;
- O QoS deve possibilitar a definição de fila de prioridade;
- Deve suportar priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
- Deve suportar marcação de pacotes DiffServ, inclusive por aplicação;

- Deve suportar modificação de valores DSCP para DiffServ;
- Deve suportar priorização de tráfego utilizando informações de ToS (Type of Service);
- Deve disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
- Deve suportar QoS (Traffic Shaping) em interfaces agregadas ou redundantes;
- Deve possibilitar a definição de bandas distintas para download e upload.

FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

- A solução deverá prover recursos de roteamento inteligente, permitindo definir, mediante regras pré-estabelecidas, o melhor caminho para o encaminhamento do tráfego das aplicações.
- A solução deverá ser capaz de agregar múltiplos links WAN em uma interface virtual única.
- A solução deverá permitir a criação de políticas de roteamento inteligente com base em critérios como endereço IP de origem, grupos de usuários, endereço IP de destino, serviços em nuvem e aplicações de camada 7, incluindo, mas não se limitando a Microsoft 365 Exchange, AWS, Dropbox e similares.
- A solução deverá medir continuamente a qualidade dos links utilizando parâmetros de latência, jitter e perda de pacotes, permitindo a configuração de limites mínimos para cada métrica, que servirão como gatilho para decisões de balanceamento e roteamento de tráfego.
- A solução deverá permitir a atualização manual ou automática das políticas de balanceamento em situações de alteração da largura de banda disponível nos links.
- A solução deverá monitorar a qualidade dos links e detectar falhas por meio do envio de testes ativos para servidores ou aplicações, suportando, no mínimo, os protocolos Ping, HTTP, TCP Echo, UDP Echo, DNS, TCP Connect e TWAMP (Two-Way Active Measurement Protocol). Adicionalmente, deverá suportar avaliação da qualidade de tráfego de voz baseada em MOS (Mean Opinion Score).
- A solução deverá possibilitar balanceamento de tráfego entre conexões WAN utilizando algoritmos configuráveis baseados em sessões, volume de tráfego, endereço IP de origem e destino, bem como transbordo de link (Spillover).
- A solução deverá permitir a criação de regras para definição de interfaces e respectivas prioridades para encaminhamento do tráfego de saída, observando os seguintes critérios:
- Manual: deverá permitir a atribuição manual de prioridades às interfaces.
- Melhor Qualidade: deverá permitir a priorização automática das interfaces com base na qualidade do link, considerando parâmetros configuráveis de latência, jitter, perda de pacotes ou largura de banda.
- Menor Custo: deverá permitir a priorização das interfaces com base no custo previamente atribuído, desde que atendidos os requisitos mínimos de qualidade do link.
- Balanceamento de Carga: deverá permitir a distribuição do tráfego entre todas as interfaces disponíveis, considerando algoritmos de balanceamento e os parâmetros de qualidade configurados.
- A solução deverá suportar marcação de pacotes DSCP nas políticas e regras de balanceamento de tráfego.
- A solução deverá suportar protocolos de roteamento dinâmico OSPFv2, OSPFv3, BGPv4 e BGP4+.
- A solução deverá realizar reconhecimento de aplicações em camada 7, contemplando, no mínimo, 3.000 (três mil) aplicações distintas, incluindo aplicações SaaS, serviços em nuvem e aplicações multimídia, tais como Vimeo, YouTube, Facebook e equivalentes.
- A solução deverá possibilitar a agregação de túneis IPsec, realizando balanceamento de tráfego por pacote entre os túneis configurados.
- A solução deverá permitir a criação dinâmica de túneis VPN entre unidades remotas, possibilitando comunicação direta entre filiais para aplicações sensíveis, sem a necessidade de encaminhamento do tráfego pela unidade sede.
- A solução deverá permitir a duplicação de pacotes por meio de dois ou mais links que atendam aos parâmetros de qualidade definidos, visando aumentar a confiabilidade e a experiência dos usuários.
- A solução deverá possuir mecanismo de correção antecipada de erros (FEC – Forward Error Correction), mediante envio de informações redundantes através de túneis VPN para compensar eventuais perdas de pacotes durante a transmissão.
- A solução deverá permitir a configuração do intervalo de verificação do estado dos links e da quantidade de

falhas necessárias para que um link seja considerado inativo, possibilitando a identificação de oscilações que possam impactar os serviços e a experiência dos usuários.

- A solução deverá suportar, nativamente, conectores para integração com provedores de nuvem pública.
- A solução deverá permitir a configuração independente das larguras de banda de download e upload em cada interface.
- A solução deverá fornecer estatísticas em tempo real referentes à utilização de banda (upload e download) e à qualidade dos links, incluindo indicadores de perda de pacotes, jitter e latência.
  A solução deverá implementar balanceamento de links utilizando algoritmo baseado em hash do endereço IP de origem.
- A solução deverá implementar balanceamento de links utilizando algoritmo baseado em hash dos endereços IP de origem e destino.
- A solução deverá implementar balanceamento por peso, permitindo definir o percentual de tráfego destinado a cada link. Deverá suportar balanceamento simultâneo de, no mínimo, três links WAN.
- O appliance físico deverá ser compatível com modems USB 3G/4G ou superior, permitindo sua utilização como link principal ou como link de contingência (standby), acionado automaticamente em caso de indisponibilidade do circuito principal.
- A solução deverá disponibilizar informações de desempenho e resultados das verificações de saúde dos links por meio de API REST, possibilitando a integração e consolidação dessas informações em plataformas de monitoramento e gestão de terceiros.

ITEM 01: CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DA SOLUÇÃO DE PROTEÇÃO DE BORDA COM NGFW “TIPO 01”, INCLUINDO IMPLANTAÇÃO, GARANTIA DO FABRICANTE, TRANSFERÊNCIA DE CONHECIMENTO E SUPORTE PELO PERÍODO DE 60 (SESSENTA) MESES

- A solução de proteção de borda baseada em Next Generation Firewall (NGFW) Tipo 01 deverá suportar throughput mínimo de 140 Gbps (cento e quarenta gigabits por segundo) com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho dos pacotes trafegados.
- A solução deverá suportar, no mínimo, 15.000.000 (quinze milhões) de conexões simultâneas.
- A solução deverá suportar, no mínimo, 685.000 (seiscentas e oitenta e cinco mil) novas conexões por segundo.
- A solução deverá suportar throughput mínimo de 50 Gbps (cinquenta gigabits por segundo) para VPN IPsec.
- A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 1.800 (mil e oitocentos) túneis VPN IPsec Site-to-Site simultâneos.
- A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 45.000 (quarenta e cinco mil) túneis simultâneos de clientes VPN IPsec.
- A solução deverá suportar throughput mínimo de 37 Gbps (trinta e sete gigabits por segundo) para a funcionalidade de Sistema de Prevenção de Intrusões (IPS).
- A solução deverá suportar throughput mínimo de 13,5 Gbps (treze vírgula cinco gigabits por segundo) para inspeção de tráfego SSL/TLS.
- A solução deverá suportar throughput mínimo de 25 Gbps (vinte e cinco gigabits por segundo) com as funcionalidades de Firewall, Controle de Aplicações, IPS e Antimalware habilitadas simultaneamente, considerando todas as assinaturas de segurança devidamente licenciadas, ativadas e em operação.
- A solução deverá possuir, no mínimo, 06 (seis) interfaces MultiGigabit Ethernet 5GBase-T com conectores RJ-45.
- A solução deverá possuir, no mínimo, 12 (doze) interfaces Gigabit Ethernet SFP.
- A solução deverá possuir, no mínimo, 04 (quatro) interfaces 10 Gigabit Ethernet SFP+.
- A solução deverá possuir, no mínimo, 04 (quatro) interfaces 25 Gigabit Ethernet SFP28.
- Deverão ser fornecidos, juntamente com cada appliance NGFW, 04 (quatro) transceptores ópticos SFP+ 10GBase-SR, do mesmo fabricante da solução ofertada.
- Deverão ser fornecidos, juntamente com cada appliance NGFW, 02 (dois) transceptores ópticos SFP28 25GBase-SR, do mesmo fabricante da solução ofertada.
- A solução deverá possuir fontes de alimentação redundantes em corrente alternada (AC), instaladas e

operacionais.

- A solução deverá estar licenciada, sem custos adicionais, para suportar, no mínimo, 10 (dez) sistemas virtuais lógicos (Virtual Systems, Contextos ou tecnologia equivalente) por appliance.

ITEM 02: CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DA SOLUÇÃO DE PROTEÇÃO DE BORDA COM NGFW "TIPO 02", INCLUINDO IMPLANTAÇÃO, GARANTIA DO FABRICANTE, TRANSFERÊNCIA DE CONHECIMENTO E SUPORTE PELO PERÍODO DE 60 (SESSENTA) MESES

- A solução de proteção de borda baseada em Next Generation Firewall (NGFW) Tipo 02 deverá suportar throughput mínimo de 26 Gbps (vinte e seis gigabits por segundo) com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho dos pacotes trafegados.
- A solução deverá suportar, no mínimo, 10.000.000 (dez milhões) de conexões simultâneas.
- A solução deverá suportar, no mínimo, 390.000 (trezentas e noventa mil) novas conexões por segundo.
- A solução deverá suportar throughput mínimo de 35 Gbps (trinta e cinco gigabits por segundo) para VPN IPsec.
- A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 1.800 (mil e oitocentos) túneis VPN IPsec Site-to-Site simultâneos.
- A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 15.000 (quinze mil) túneis simultâneos de clientes VPN IPsec.
- A solução deverá suportar throughput mínimo de 8 Gbps (oito gigabits por segundo) para a funcionalidade de Sistema de Prevenção de Intrusões (IPS).
- A solução deverá suportar throughput mínimo de 6 Gbps (seis gigabits por segundo) para inspeção de tráfego SSL/TLS.
- A solução deverá suportar throughput mínimo de 5 Gbps (cinco gigabits por segundo) com as funcionalidades de Firewall, Controle de Aplicações, IPS e Antimalware habilitadas simultaneamente, considerando todas as assinaturas de segurança devidamente licenciadas, ativadas e em operação.
- A solução deverá possuir, no mínimo, 08 (oito) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45.
- A solução deverá possuir, no mínimo, 04 (quatro) interfaces Gigabit Ethernet SFP.
- A solução deverá possuir, no mínimo, 06 (seis) interfaces 10 Gigabit Ethernet SFP+.
- Deverão ser fornecidos, juntamente com cada appliance NGFW, 04 (quatro) transceptores ópticos SFP+ 10GBase-SR, do mesmo fabricante da solução ofertada.
- A solução deverá possuir fontes de alimentação redundantes em corrente alternada (AC), instaladas e operacionais.
- A solução deverá estar licenciada, sem custos adicionais, para suportar, no mínimo, 10 (dez) sistemas virtuais lógicos (Virtual Systems, Contextos ou tecnologia equivalente) por appliance.

ITEM 03: CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DA SOLUÇÃO DE PROTEÇÃO DE BORDA COM NGFW "TIPO 03", INCLUINDO IMPLANTAÇÃO, GARANTIA DO FABRICANTE, TRANSFERÊNCIA DE CONHECIMENTO E SUPORTE PELO PERÍODO DE 60 (SESSENTA) MESES

- A solução de proteção de borda baseada em Next Generation Firewall (NGFW) Tipo 03 deverá suportar throughput mínimo de 26 Gbps (vinte e seis gigabits por segundo) com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho dos pacotes trafegados.
- A solução deverá suportar, no mínimo, 2.800.000 (dois milhões e oitocentas mil) conexões simultâneas.
- A solução deverá suportar, no mínimo, 138.000 (cento e trinta e oito mil) novas conexões por segundo.
- A solução deverá suportar throughput mínimo de 33 Gbps (trinta e três gigabits por segundo) para VPN IPsec.
- A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 1.800 (mil e oitocentos) túneis VPN IPsec Site-to-Site simultâneos.
- A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 15.000 (quinze mil) túneis simultâneos de clientes VPN IPsec.
- A solução deverá suportar throughput mínimo de 5 Gbps (cinco gigabits por segundo) para a funcionalidade de Sistema de Prevenção de Intrusões (IPS).

- A solução deverá suportar throughput mínimo de 2,8 Gbps (dois vírgula oito gigabits por segundo) para inspeção de tráfego SSL/TLS.
- A solução deverá suportar throughput mínimo de 2,7 Gbps (dois vírgula sete gigabits por segundo) com as funcionalidades de Firewall, Controle de Aplicações, IPS e Antimalware habilitadas simultaneamente, considerando todas as assinaturas de segurança devidamente licenciadas, ativadas e em operação.
- A solução deverá possuir, no mínimo, 12 (doze) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45.
- A solução deverá possuir, no mínimo, 08 (oito) interfaces Gigabit Ethernet SFP.
- A solução deverá possuir, no mínimo, 04 (quatro) interfaces 10 Gigabit Ethernet SFP+.
- Deverão ser fornecidos, juntamente com cada appliance NGFW, 04 (quatro) transceptores ópticos SFP+ 10GBase-SR, do mesmo fabricante da solução ofertada.
- A solução deverá possuir fontes de alimentação redundantes em corrente alternada (AC), instaladas e operacionais.
- A solução deverá estar licenciada, sem custos adicionais, para suportar, no mínimo, 10 (dez) sistemas virtuais lógicos (Virtual Systems, Contextos ou tecnologia equivalente) por appliance.

ITEM 04: CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DA SOLUÇÃO DE PROTEÇÃO DE BORDA COM NGFW "TIPO 04", INCLUINDO IMPLANTAÇÃO, GARANTIA DO FABRICANTE, TRANSFERÊNCIA DE CONHECIMENTO E SUPORTE PELO PERÍODO DE 60 (SESSENTA) MESES

- A solução de proteção de borda baseada em Next Generation Firewall (NGFW) Tipo 04 deverá suportar throughput mínimo de 24 Gbps (vinte e quatro gigabits por segundo) com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho dos pacotes trafegados.
- A solução deverá suportar, no mínimo, 2.700.000 (dois milhões e setecentas mil) conexões simultâneas.
- A solução deverá suportar, no mínimo, 120.000 (cento e vinte mil) novas conexões por segundo.
- A solução deverá suportar throughput mínimo de 24 Gbps (vinte e quatro gigabits por segundo) para VPN IPsec.
- A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 180 (cento e oitenta) túneis VPN IPsec Site-to-Site simultâneos.
- A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 2.000 (dois mil) túneis simultâneos de clientes VPN IPsec.
- A solução deverá suportar throughput mínimo de 4,3 Gbps (quatro vírgula três gigabits por segundo) para a funcionalidade de Sistema de Prevenção de Intrusões (IPS).
- A solução deverá suportar throughput mínimo de 2,4 Gbps (dois vírgula quatro gigabits por segundo) para inspeção de tráfego SSL/TLS.
- A solução deverá suportar throughput mínimo de 2 Gbps (dois gigabits por segundo) com as funcionalidades de Firewall, Controle de Aplicações, IPS e Antimalware habilitadas simultaneamente, considerando todas as assinaturas de segurança devidamente licenciadas, ativadas e em operação.
- A solução deverá possuir, no mínimo, 06 (seis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45.
- A solução deverá possuir, no mínimo, 02 (duas) interfaces MultiGigabit Ethernet 5GBase-T com conectores RJ-45.
- A solução deverá estar licenciada, sem custos adicionais, para suportar, no mínimo, 10 (dez) sistemas virtuais lógicos (Virtual Systems, Contextos ou tecnologia equivalente) por appliance.

ITEM 05: CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DA SOLUÇÃO DE PROTEÇÃO DE BORDA COM NGFW "TIPO 05", INCLUINDO IMPLANTAÇÃO, GARANTIA DO FABRICANTE, TRANSFERÊNCIA DE CONHECIMENTO E SUPORTE PELO PERÍODO DE 60 (SESSENTA) MESES

- A solução de proteção de borda baseada em Next Generation Firewall (NGFW) Tipo 05 deverá suportar throughput mínimo de 9 Gbps (nove gigabits por segundo) com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independentemente do tamanho dos pacotes trafegados.
- A solução deverá suportar, no mínimo, 1.200.000 (um milhão e duzentas mil) conexões simultâneas.
- A solução deverá suportar, no mínimo, 90.000 (noventa mil) novas conexões por segundo.
- A solução deverá suportar throughput mínimo de 7 Gbps (sete gigabits por segundo) para VPN IPsec.

- A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 160 (cento e sessenta) túneis VPN IPsec Site-to-Site simultâneos.
- A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 400 (quatrocentos) túneis simultâneos de clientes VPN IPsec.
- A solução deverá suportar throughput mínimo de 2,4 Gbps (dois vírgula quatro gigabits por segundo) para a funcionalidade de Sistema de Prevenção de Intrusões (IPS).
- A solução deverá suportar throughput mínimo de 1,2 Gbps (um vírgula dois gigabits por segundo) para inspeção de tráfego SSL/TLS.
- A solução deverá suportar throughput mínimo de 1,2 Gbps (um vírgula dois gigabits por segundo) com as funcionalidades de Firewall, Controle de Aplicações, IPS e Antimalware habilitadas simultaneamente, considerando todas as assinaturas de segurança devidamente licenciadas, ativadas e em operação.
- A solução deverá possuir, no mínimo, 06 (seis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45.
- A solução deverá estar licenciada, sem custos adicionais, para suportar, no mínimo, 10 (dez) sistemas virtuais lógicos (Virtual Systems, Contextos ou tecnologia equivalente) por appliance.

ITEM 06: SOLUÇÃO DE GESTÃO DE LOGS E RELATÓRIOS PARA AMBIENTE UNIFICADO DE NGFW, COM CAPACIDADE DE 25 GB/DIA DE LOGS, INCLUINDO IMPLANTAÇÃO, GARANTIA DO FABRICANTE, TRANSFERÊNCIA DE CONHECIMENTO E SUPORTE PELO PERÍODO DE 60 (SESSENTA) MESES

- Deverá ser fornecida solução de gerenciamento de logs e geração de relatórios para todos os appliances disponibilizados nos Itens 01, 02, 03, 04 e 05, incluindo implantação, garantia do fabricante, transferência de conhecimento e suporte técnico pelo período de 60 (sessenta) meses.
- A implantação deverá ser realizada presencialmente por profissional certificado pelo fabricante, nas dependências da CONTRATANTE.
- A solução deverá ser do mesmo fabricante das soluções especificadas nos Itens 01, 02, 03, 04, 05 e 07 deste Termo de Referência.
- A solução deverá suportar acesso para gerenciamento por meio dos protocolos SSH e HTTPS.
- A solução de gerenciamento centralizado deverá ser disponibilizada na forma de appliance virtual, sendo de responsabilidade da CONTRATANTE o fornecimento dos recursos de hardware e da plataforma de virtualização necessários para sua operação.
- A solução deverá ser compatível, no mínimo, com os hypervisores VMware ESXi, Microsoft Hyper-V 2016, 2019 e 2022, Red Hat Virtualization, Nutanix AHV e Linux KVM.
- A solução deverá possuir licenciamento perpétuo, contemplando suporte do fabricante por período mínimo de 60 (sessenta) meses.
- Na data de apresentação da proposta, o modelo ofertado não poderá constar em listas de End of Sale (EOS) ou End of Life (EOL) divulgadas pelo fabricante.
- A solução não deverá impor limitação quanto à quantidade de vCPUs suportadas.
- A solução não deverá impor limitação quanto à expansão de memória RAM.
- A solução virtual não deverá impor limitação de armazenamento além da capacidade disponibilizada pelos discos alocados à máquina virtual.
- A solução deverá permitir acesso simultâneo de administradores e possibilitar a criação de, no mínimo, 02 (dois) perfis distintos para administração e monitoramento.
- A solução deverá suportar os protocolos SNMP versões 2 e 3.
- A solução deverá permitir a virtualização do gerenciamento dos dispositivos, garantindo que cada administrador tenha acesso apenas aos equipamentos sob sua responsabilidade.
- A solução deverá permitir a criação de administrador global com acesso irrestrito a todas as instâncias virtualizadas da plataforma.
- A solução deverá suportar perfis de acesso com permissões granulares, incluindo leitura, gravação, criação de usuários e alteração de configurações gerais.
- A solução deverá suportar autenticação de usuários por LDAP, RADIUS e TACACS+.

- A solução deverá suportar configuração de alta disponibilidade (HA) em arquitetura Master/Slave em camada 3.
- A solução deverá permitir a geração de alertas baseados nos eventos registrados nos logs.
- A solução deverá disponibilizar relatórios predefinidos.
- A solução deverá permitir a importação e exportação de relatórios.
- A solução deverá suportar geração de relatórios de tráfego em tempo real em formato de mapa geográfico.
- A solução deverá suportar geração de relatórios de tráfego em tempo real em formato de gráfico de bolhas.
- A solução deverá suportar geração de relatórios de tráfego em tempo real em formato de tabela gráfica.
- A solução deverá permitir a personalização de gráficos dos relatórios, incluindo gráficos de barras, linhas e tabelas.
- A solução deverá permitir a personalização da capa dos relatórios.
- A solução deverá permitir a geração e envio automático de relatórios periódicos.
- A solução deverá permitir a geração de relatórios nos formatos HTML, CSV, XML e PDF.
- A solução deverá possuir assistente gráfico para inclusão de novos dispositivos por meio de endereço IP, usuário e senha.
- A solução deverá permitir visualizar a quantidade de logs enviados por cada dispositivo monitorado.
- A solução deverá possuir mecanismos automáticos de remoção de logs antigos.
- A solução deverá disponibilizar recurso de pesquisa detalhada (Drill-Down) para navegação em relatórios em tempo real.
- A solução deverá permitir a personalização de relatórios predefinidos pelo administrador.
- A solução deverá permitir o envio automático de relatórios por correio eletrônico.
- A solução deverá permitir o envio de relatórios para destinatários específicos.
- A solução deverá permitir o agendamento da geração de relatórios conforme calendário definido pelo administrador.
- A solução deverá permitir a visualização gráfica e em tempo real da taxa de geração de logs de cada dispositivo gerenciado.
- A solução deverá permitir a aplicação de filtros nos relatórios.
- A solução deverá permitir a customização completa do layout dos relatórios, incluindo gráficos, textos, imagens, alinhamentos, fontes, cores e quebras de página.
- A solução deverá permitir a definição do idioma dos relatórios gerados.
- A solução deverá gerar alertas automáticos via e-mail, SNMP e Syslog com base em eventos, severidade e critérios definidos pelo administrador.
- A solução deverá permitir o envio automático de relatórios para servidores externos via SFTP ou FTP.
- A solução deverá permitir o envio automático dos logs para servidores FTP externos.
- A solução deverá permitir a exportação de logs em formato CSV.
- A solução deverá permitir o download dos arquivos de log para utilização externa.
- A solução deverá gerar logs de auditoria contendo detalhes das alterações realizadas, identificação do administrador responsável e registro de data e hora.
- Os logs dos dispositivos gerenciados deverão ser centralizados na plataforma, devendo a solução também permitir integração com servidores Syslog externos ou tecnologias equivalentes.
- A solução deverá permitir a criação de consultas SQL ou tecnologia equivalente nos bancos de dados de logs para utilização em gráficos e relatórios.
- A interface gráfica deverá exibir informações do sistema, incluindo licenciamento, utilização de memória, armazenamento, CPU, taxa de logs por segundo, total diário de logs e alertas do sistema.
- A solução deverá fornecer informações sobre quantidade de logs armazenados e estimativa de retenção disponível.
- A solução deverá permitir a definição de políticas de senha para administradores, incluindo tamanho mínimo e requisitos de complexidade.

- A solução deverá permitir a visualização em tempo real dos logs recebidos.
- A solução deverá suportar encaminhamento de logs nos formatos Syslog e CEF (Common Event Format).
- A solução deverá permitir a visualização centralizada dos logs provenientes de um ou mais dispositivos, incluindo mecanismos de filtragem para facilitar pesquisas.
- Os logs de auditoria e alterações de configuração deverão ser exibidos separadamente dos logs de tráfego de rede.
- A solução deverá possuir painel operacional para monitoramento das principais ameaças de segurança da rede.
- A solução deverá possuir painel operacional para monitoramento do comportamento dos usuários e identificação de utilização suspeita da web.
- A solução deverá possuir painel operacional para monitoramento do tráfego de rede, aplicações e navegação web.
- A solução deverá possuir painel operacional para monitoramento da atividade de VPN.
- A solução deverá possuir painel operacional para monitoramento dos recursos locais da plataforma, incluindo CPU e memória.
- A solução deverá permitir a criação de painéis personalizados para monitoramento de operações de rede e segurança.
- A solução deverá disponibilizar relatórios de utilização de aplicações e mídias sociais.
- A solução deverá disponibilizar relatórios de prevenção contra perda de dados (DLP).
- A solução deverá disponibilizar relatórios de VPN, IPS e análise de ameaças cibernéticas.
- A solução deverá disponibilizar relatório resumido diário de eventos e incidentes de segurança.
- A solução deverá disponibilizar relatório de tráfego DNS e correio eletrônico.
- A solução deverá disponibilizar relatório das 10 (dez) aplicações mais utilizadas na rede.
- A solução deverá disponibilizar relatório dos 10 (dez) principais sites acessados na rede.
- A solução deverá fornecer visibilidade sobre a utilização dos recursos de balanceamento inteligente de links (SD-WAN), incluindo uso das regras por aplicação, consumo de banda e indicadores de qualidade dos links, tais como latência, jitter e perda de pacotes.
- A solução deverá permitir, por meio da análise de tráfego IP, URLs e domínios acessados, identificar equipamentos potencialmente comprometidos ou usuários com comportamento suspeito.
- A solução deverá permitir a atribuição de pontuações de risco baseadas na análise de tráfego IP, URLs e domínios acessados, classificando os níveis de comprometimento em baixo, médio e alto.
- A solução deverá permitir análise detalhada de dispositivos comprometidos, apresentando informações completas sobre as ameaças identificadas.
- A solução deverá suportar recursos de automação (playbooks), integrando-se a soluções de firewall, endpoint, correio eletrônico, ITSM e eventos predefinidos para execução automática de ações de mitigação.
- A solução deverá suportar correlação de eventos, disponibilizando painéis analíticos e permitindo a criação de novas visualizações para recursos de rede e segurança.
- A solução deverá suportar recebimento de, no mínimo, 25 GB (vinte e cinco gigabytes) de logs por dia.
- A solução deverá suportar integralmente a capacidade diária de armazenamento e processamento de logs especificada neste item, sem degradação de desempenho.

ITEM 07: SOLUÇÃO DE GESTÃO CENTRALIZADA DE AMBIENTE UNIFICADO DE NGFW, COM IMPLANTAÇÃO, GARANTIA DO FABRICANTE, TRANSFERÊNCIA DE CONHECIMENTO E SUPORTE, PARA ATÉ 10 (DEZ) DISPOSITIVOS FÍSICOS, PELO PERÍODO DE 60 (SESSENTA) MESES

CARACTERÍSTICAS PARA GERENCIAMENTO CENTRALIZADO

- Deverá ser fornecida solução de gerenciamento centralizado para todos os appliances disponibilizados nos Itens 01, 02, 03, 04 e 05, incluindo implantação, garantia do fabricante, transferência de conhecimento e suporte técnico pelo período de 60 (sessenta) meses.
- A solução deverá ser do mesmo fabricante das soluções especificadas nos Itens 01, 02, 03, 04, 05 e 06 deste

Termo de Referência.

- A solução deverá possuir licenciamento perpétuo, contemplando suporte do fabricante por período mínimo de 60 (sessenta) meses.
- A implantação deverá ser realizada presencialmente por profissional certificado pelo fabricante, nas dependências da CONTRATANTE.
- A solução deverá estar dimensionada e licenciada para gerenciar até 10 (dez) Firewalls de Próxima Geração (NGFW), considerando os modelos ofertados para os Tipos 01, 02, 03, 04 e 05, atendendo integralmente aos requisitos deste item.
- A solução de gerenciamento centralizado deverá ser disponibilizada na forma de appliance virtual, sendo de responsabilidade da CONTRATANTE o fornecimento dos recursos de hardware e software (hypervisor) necessários ao seu funcionamento.
- A solução deverá ser compatível, no mínimo, com os hypervisores VMware ESXi, Microsoft Hyper-V 2016, 2019 e 2022, Red Hat Virtualization, Nutanix AHV e Linux KVM.
- Na data de apresentação da proposta, o modelo ofertado não poderá constar em listas de End of Sale (EOS) ou End of Life (EOL) divulgadas pelo fabricante.
- A solução não deverá impor limitação quanto à quantidade de vCPUs suportadas.
- A solução não deverá impor limitação quanto à expansão de memória RAM.
- A solução deverá possibilitar a criação e administração centralizada de políticas de Firewall, Controle de Aplicações, Sistema de Prevenção de Intrusão (IPS), Antivírus, Filtro de Conteúdo e URL, bem como Balanceamento Inteligente de Links (SD-WAN).
- A solução deverá fornecer visibilidade centralizada das verificações de saúde dos links, desempenho das aplicações, utilização de largura de banda e conformidade com os níveis de serviço definidos.
- A solução deverá permitir o provisionamento centralizado de comunidades VPN, o monitoramento das conexões VPN de todos os dispositivos gerenciados e a exibição geográfica dessas conexões em mapa.
- A solução deverá permitir a criação de templates de configuração contendo parâmetros de DNS, SNMP, logs e administração dos dispositivos.
- A solução deverá suportar arquitetura multi-tenant, permitindo o gerenciamento de ambientes independentes por meio de uma única plataforma.
- A solução deverá disponibilizar APIs RESTful para integração com portais personalizados e automação da configuração de objetos e políticas de segurança.
- A solução deverá garantir a integridade das configurações mediante mecanismo de bloqueio de alterações quando houver acesso simultâneo de múltiplos administradores ao mesmo ativo.
- A solução deverá permitir acesso concorrente de administradores e possibilitar a definição de fluxo de aprovação para alterações realizadas.
- A solução deverá permitir a criação de perfis de acesso com permissões granulares, incluindo leitura, escrita, criação de usuários e alteração de configurações.
- A solução deverá permitir a utilização de palavras-chave, etiquetas ou cores para facilitar a identificação de regras.
- A solução deverá permitir localizar todas as regras em que determinado objeto esteja sendo utilizado.
- A solução deverá atribuir numeração sequencial às regras de Firewall, NAT e QoS.
- A solução deverá permitir a criação de regras com vigência condicionada a horários específicos.
- A solução deverá permitir a criação de regras com data de expiração definida.
- A solução deverá realizar cópias de segurança das configurações, permitindo a restauração de versões previamente armazenadas.
- A solução deverá possuir mecanismo de validação de políticas capaz de identificar conflitos, redundâncias ou sobreposição de regras, ou tecnologia equivalente que atenda plenamente a esse requisito.
- A solução deverá gerar alertas automáticos por e-mail, SNMP e Syslog.
- A solução deverá permitir a transferência de backups para servidores FTP, SCP ou SFTP.
- A solução deverá permitir a realização de backup e rollback das configurações para versões anteriormente

salvas.

- A solução deverá possibilitar a visualização e comparação entre configurações atuais e versões anteriores.
- A solução deverá possuir mecanismo completo de backup e restauração de suas configurações, permitindo também o agendamento automático dos processos de backup.
- A solução deverá suportar a distribuição e instalação remota e centralizada de novas versões de software dos equipamentos gerenciados.
- A solução deverá permitir a criação centralizada de objetos utilizados nas políticas de segurança.
- A solução deverá suportar autenticação de administradores por base local e por serviços externos utilizando RADIUS, LDAP, TACACS+ e infraestrutura de chaves públicas (PKI).
- A solução deverá incluir ferramenta para gerenciamento centralizado das licenças de todos os appliances administrados, permitindo a atualização das licenças diretamente pela plataforma.
- A solução deverá possibilitar a distribuição e instalação remota, centralizada e automatizada de novas versões de software dos appliances gerenciados.
- A solução deverá suportar o gerenciamento centralizado de pontos de acesso sem fio (Access Points).
- A solução deverá suportar o gerenciamento centralizado de switches.
- A solução deverá contemplar garantia, suporte técnico e direito a atualizações de software durante toda a vigência contratual de 60 (sessenta) meses.

ITEM 8 - UNIDADES DE SERVIÇOS TÉCNICOS – USTs

- A Unidade de Serviço Técnico – UST constitui unidade de medição destinada à remuneração de serviços técnicos especializados efetivamente executados e entregues pela CONTRATADA, vinculados ao objeto desta contratação, mediante resultados, produtos ou atividades previamente definidos no Catálogo de Serviços.
- A utilização das USTs não caracteriza contratação ou disponibilização de mão de obra por tempo determinado, nem remuneração por horas trabalhadas, devendo o pagamento estar vinculado à efetiva execução e entrega dos serviços solicitados e devidamente atestados pela CONTRATANTE.
- A CONTRATANTE poderá utilizar até 4.000 (quatro mil) USTs durante a vigência contratual, destinadas à execução de serviços técnicos especializados relacionados à infraestrutura de tecnologia da informação, redes, segurança da informação e segurança cibernética, desde que vinculados ao objeto deste Termo de Referência.
- As USTs poderão ser utilizadas durante o período de vigência contratual, de acordo com a necessidade da CONTRATANTE, não havendo obrigação de consumo mínimo, pagamento antecipado ou garantia de utilização da totalidade das unidades previstas.
- A solicitação dos serviços será formalizada mediante Ordem de Serviço – OS, emitida pela CONTRATANTE, contendo, no mínimo, a descrição da demanda, o serviço a ser executado, a quantidade de USTs prevista no Catálogo de Serviços, os requisitos técnicos, os critérios de aceite e, quando aplicável, a prioridade e o prazo para execução.
- A quantidade de USTs correspondente a cada serviço será aquela previamente estabelecida no Catálogo de Serviços de Referência, constante deste Termo de Referência, não cabendo à CONTRATADA definir unilateralmente o quantitativo a ser consumido para a execução da demanda.
- Os serviços serão classificados pela CONTRATANTE quanto ao grau de urgência e, quando necessário, quanto à complexidade, exclusivamente para fins de priorização, planejamento e definição do prazo de atendimento, não implicando alteração do quantitativo de UST previamente estabelecido para o serviço no Catálogo de Serviços.
- A CONTRATADA deverá executar os serviços de acordo com as especificações constantes da Ordem de Serviço, observando os requisitos técnicos, os critérios de aceite, as boas práticas de mercado, as recomendações dos fabricantes e as normas de segurança da informação aplicáveis.
- A execução dos serviços poderá ocorrer de forma presencial, remota ou híbrida, conforme a natureza da demanda e a necessidade da CONTRATANTE.
- Concluído o serviço, a CONTRATADA deverá apresentar, no prazo máximo de 02 (dois) dias úteis, relatório técnico contendo, no mínimo, a descrição das atividades realizadas, os procedimentos adotados,

os resultados obtidos, os produtos ou entregáveis disponibilizados e as evidências necessárias à comprovação da execução.

- O pagamento será realizado exclusivamente após a conclusão do serviço, a verificação do cumprimento dos requisitos estabelecidos na respectiva Ordem de Serviço e o aceite pela CONTRATANTE, observando-se o quantitativo de UST previamente definido no Catálogo de Serviços.
- Caso o serviço executado não atenda aos requisitos ou critérios de aceite estabelecidos na Ordem de Serviço, a CONTRATADA deverá realizar as correções necessárias, sem acréscimo de USTs, até que sejam atendidas as condições estabelecidas para o aceite.
- A CONTRATADA deverá disponibilizar profissionais tecnicamente qualificados e habilitados para a execução dos serviços previstos, responsabilizando-se integralmente pelos recursos humanos necessários à entrega dos resultados contratados.
- A execução dos serviços poderá ocorrer durante o horário comercial ou fora dele, conforme a criticidade da demanda e a necessidade da CONTRATANTE, especialmente em situações que envolvam indisponibilidade, incidentes de segurança ou riscos à continuidade dos serviços institucionais.

CATÁLOGO DE SERVIÇOS DE REFERÊNCIA

- Para fins de padronização da medição e remuneração dos serviços, a CONTRATANTE adotará Catálogo de Serviços de Referência, contendo a descrição dos serviços, os respectivos produtos ou resultados esperados e o quantitativo de USTs correspondente a cada serviço.
- O Catálogo de Serviços constitui referência objetiva para a emissão das Ordens de Serviço e para a medição dos serviços executados, buscando assegurar previsibilidade, padronização, transparência e vinculação da remuneração aos resultados efetivamente entregues.
- **O Catálogo de Serviços contemplará, no mínimo, os seguintes serviços:**

CÓD.	SERVIÇO	RESULTADO/ENTREGÁVEL ESPERADO	UST
UST-01	Diagnóstico e troubleshooting de firewall	Relatório técnico com diagnóstico, causa identificada e solução aplicada ou recomendada	10
UST-02	Configuração ou alteração de regra de firewall	Regra implementada, validada e documentada	4
UST-03	Criação, alteração ou exclusão de objeto de rede	Objeto configurado e validado no equipamento	2
UST-04	Liberação ou bloqueio de IP, porta ou serviço	Regra implementada e validada	2
UST-05	Configuração de NAT	Configuração implementada, testada e documentada	4
UST-06	Configuração de VPN	Túnel VPN configurado, testado e documentado	8
UST-07	Análise de logs e eventos de segurança	Relatório técnico com análise, evidências e recomendações	6
UST-08	Análise e tratamento de incidente de segurança	Diagnóstico, tratamento, evidências e relatório técnico	12
UST-09	Análise de vulnerabilidade	Relatório contendo vulnerabilidades identificadas, classificação e recomendações	10
UST-10	Aplicação de atualização de firmware/software	Atualização executada, validada e documentada	8
UST-11	Ajuste de políticas de segurança	Políticas revisadas, implementadas, testadas e documentadas	8
UST-12	Teste de contingência e alta disponibilidade	Teste realizado, resultados registrados e relatório apresentado	12
UST-13	Teste de restauração de configuração	Restauração executada e validada, com evidências	6
UST-14	Otimização de desempenho da solução	Análise, ajustes realizados e relatório de desempenho	10

CÓD.	SERVIÇO	RESULTADO/ENTREGÁVEL ESPERADO	UST
UST-15	Elaboração ou atualização de documentação técnica	Documento técnico atualizado e entregue	6
UST-16	Consultoria técnica especializada	Análise técnica formalizada e apresentação das recomendações	8
UST-17	Treinamento técnico	Capacitação realizada e material disponibilizado	10
UST-18	Avaliação de segurança cibernética	Avaliação realizada, evidências coletadas e relatório técnico apresentado	20
UST-19	Teste de intrusão (Pentest)	Execução do teste e entrega de relatório técnico com vulnerabilidades e recomendações	30
UST-20	Atividade técnica especializada não prevista no catálogo	Serviço previamente especificado e aprovado pela CONTRATANTE, com definição prévia do quantitativo de UST	A definir previamente

- Os quantitativos de UST previstos no Catálogo de Serviços correspondem à complexidade técnica e ao conjunto de atividades necessárias para a obtenção dos respectivos resultados ou entregáveis, não representando quantidade de horas de trabalho ou tempo de disponibilização de profissionais.
- Para os serviços previstos no Catálogo, a quantidade de UST será fixa, não podendo ser alterada unilateralmente pela CONTRATADA em razão do tempo efetivamente empregado na execução.
- Nas situações em que a demanda envolver mais de um serviço previsto no Catálogo, a Ordem de Serviço deverá discriminar os serviços a serem executados e o respectivo quantitativo de UST, permitindo a apuração objetiva do valor devido.
- Para demandas que não estejam expressamente previstas no Catálogo de Serviços, a CONTRATADA deverá apresentar proposta técnica contendo a descrição do serviço, os resultados esperados, os produtos ou entregáveis e a quantidade de USTs necessária, cabendo à CONTRATANTE avaliar e aprovar previamente o quantitativo antes do início da execução.
- A aprovação prevista no subitem anterior deverá ser formalizada pela CONTRATANTE, não sendo devido qualquer pagamento por serviço executado sem prévia autorização.

DA URGÊNCIA E PRIORIZAÇÃO

- As demandas poderão ser classificadas pela CONTRATANTE, conforme sua criticidade, nos níveis de prioridade Alta, Média ou Baixa.
- A classificação de prioridade será utilizada exclusivamente para estabelecer a ordem de atendimento e o prazo de execução da demanda, não alterando o quantitativo de UST estabelecido no Catálogo de Serviços.
- Considera-se, exemplificativamente, como prioridade Alta, a indisponibilidade total de equipamento ou serviço de segurança de rede, incidente de segurança cibernética com impacto institucional relevante ou situação que comprometa a continuidade de serviços essenciais.
- Considera-se prioridade Média aquela relacionada a degradação parcial de serviços, necessidade de ajustes de configuração, manutenção ou correções que não impliquem indisponibilidade total da solução.
- Considera-se prioridade Baixa aquela relacionada a atividades de melhoria, otimização, documentação, consultoria, ajustes não críticos ou demandas programáveis.

DO CONTROLE E ATESTO

- A CONTRATANTE manterá controle das USTs autorizadas, executadas, aceitas e pagas, de forma a possibilitar o acompanhamento do saldo contratual e a rastreabilidade das demandas.
- A CONTRATADA deverá apresentar, até o 5º (quinto) dia útil do mês subsequente, relatório consolidado contendo as Ordens de Serviço executadas no período, os serviços realizados, os respectivos resultados ou entregáveis, as USTs utilizadas e a situação de aceite de cada demanda.
- O fiscal do contrato verificará a conformidade dos serviços executados com as respectivas Ordens de

Serviço e critérios de aceite, promovendo o atesto somente após a comprovação da efetiva entrega dos resultados contratados.

- Não serão computadas ou remuneradas USTs relativas a atividades que não tenham sido previamente autorizadas, que não estejam vinculadas ao objeto contratado ou que não tenham sido efetivamente executadas e aceitas pela CONTRATANTE.
- As USTs previstas no contrato constituem limite máximo de consumo, não gerando direito adquirido da CONTRATADA ao seu consumo integral.

Referências:

1. ^ **Next Generation Firewall (NGFW)** é uma evolução dos firewalls tradicionais. Além de controlar o tráfego com base em IP, portas e protocolos, ele inspeciona o conteúdo dos dados e identifica aplicações, usuários e ameaças em tempo real.
2. ^ **Deep Packet Inspection (DPI)** é uma tecnologia de análise de rede que examina não apenas os cabeçalhos dos pacotes de dados, mas também o conteúdo (payload) transportado por eles.
3. ^ O **IPS (Intrusion Prevention System)** é uma solução de segurança que monitora o tráfego de rede em tempo real para identificar e bloquear atividades maliciosas antes que causem danos aos sistemas.
4. ^ Uma **VPN (Virtual Private Network)** é uma tecnologia que cria uma conexão segura e criptografada através de uma rede pública, como a Internet, permitindo a troca de dados com privacidade e segurança.
5. ^ A **Lei Geral de Proteção de Dados Pessoais (LGPD)** é a legislação brasileira que estabelece regras para a coleta, armazenamento, utilização, compartilhamento e eliminação de dados pessoais por organizações públicas e privadas. Seu principal objetivo é proteger a privacidade, a liberdade e os direitos fundamentais dos cidadãos
6. ^ **SSL/TLS Inspection** é uma tecnologia de segurança que permite analisar o tráfego criptografado por SSL/TLS (como conexões HTTPS) para identificar ameaças, malwares, vazamento de dados ou atividades suspeitas que estariam ocultas pela criptografia.
7. ^ **High Availability (HA)** ou **Alta Disponibilidade** é uma arquitetura projetada para manter sistemas, serviços ou aplicações operando continuamente, minimizando interrupções e reduzindo o tempo de indisponibilidade.

Documento assinado eletronicamente por **rogerio leite moresco**, **Assessor Técnico**, em 14/09/2026, às 10:09, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.ap.def.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0270399** e o código CRC **2B978BC6**.
