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

ESTUDO TÉCNICO PRELIMINAR

1. INFORMAÇÕES BÁSICAS

1.1. Processo n.º SEI n.º **26.0.000003969-0**

1.2. Número da Contratação PCA: UASG 927560, Documento de Formalização **27/2026.**

2. OBJETO

2.1. Contratação de solução de segurança de rede do tipo **Next Generation Firewall (NGFW)**, 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.

3. ORIGEM DA DEMANDA

3.2. Esta peça é elaborada com base no §1º, art. 18 da Lei Federal nº 14.133/2021, §3º do art. 1º da Portaria nº 37 e 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)*, constituindo a primeira etapa do planejamento da contratação, a fim de avaliar a melhor solução disponível no mercado para atender a necessidade deste órgão e assegurar a sua viabilidade técnica, econômica e de gestão, bem como dar suporte à elaboração do Termo de Referência.

4. DESCRIÇÃO DA NECESSIDADE

4.1. 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.

4.2. 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.

4.3. 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.

4.4. 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.

4.5. 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.

4.6. 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.

4.7. 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), sistema de prevenção de intrusão (IPS), 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) seguras e mecanismos de alta disponibilidade.

4.8. 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.

4.9. A contratação também visa assegurar a continuidade dos serviços de suporte técnico, garantia, 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.

4.10. A presente contratação está alinhada aos princípios da eficiência, continuidade do serviço público 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.

4.11. Adicionalmente, a contratação atende às diretrizes estabelecidas pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que impõe aos órgãos públicos o dever de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, perda, alteração, divulgação ou qualquer forma de tratamento inadequado ou ilícito.

4.12. Diante desse cenário, o presente Estudo Técnico Preliminar busca avaliar as alternativas disponíveis no mercado e identificar a solução que melhor atenda às necessidades institucionais, observando critérios de desempenho, segurança, escalabilidade, suporte técnico, eficiência operacional e vantajosidade para a Administração Pública.

4.13. 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.

5. ÁREA REQUISITANTE

5.1.

Área Requisitante	Responsável	Cargo	Portaria
Coordenadoria de Tecnologia da Informação	Walter da Silva Araújo Filho	Coordenador de Tecnologia da Informação	Portaria nº 108, de 24 de janeiro de 2024

6. REQUISITOS DA CONTRATAÇÃO

6.1. Requisitos de Negócio

6.1.1. 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.

6.1.2. 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.

6.1.3. 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.

6.1.4. 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.

6.1.5. 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.

6.1.6. 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.

6.1.7. 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.

6.1.8. 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.

6.2. Requisitos Legais

6.2.1. 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 37, de 10 de Janeiro de 2024 (Regulamenta a elaboração de Estudos Técnicos Preliminares - ETP e alterações no âmbito da Defensoria Pública do Estado do Amapá,)

6.3. Requisitos Temporais

6.3.1. 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, seguinda 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.

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

6.3.2.1. 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.

6.3.2.2. 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 inculcalíveis, alheios à sua vontade, que comprovadamente impeçam ou dificultem o cumprimento do prazo originalmente estabelecido.

6.3.2.3. 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.

6.3.2.4. 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.

6.3.2.5. 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.

6.3.2.6. 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.

6.3.2.7. 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.

6.4. Requisitos Sociais, Ambientais e Culturais

6.4.1. 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.

6.4.2. 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).

6.4.3. 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).

6.4.4. Seguindo a lógica do item 6.4.1., 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.

6.4.5. 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.

6.5. Requisitos Tecnológicos para Infraestrutura de Firewall

6.5.1. 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.

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

6.5.3. 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.

6.5.4. 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.

6.5.5. 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.

6.5.6. 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.

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

6.5.8. 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.

6.5.9. 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.

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

6.5.11. 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.

6.5.12. 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.

6.6. Requisitos de Instalação e Configuração

6.6.1. 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.

6.6.2. 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.

6.6.3. 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.

6.6.4. 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.

6.6.5. 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.

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

6.6.7. 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.

6.6.8. 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.

6.6.9. 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.

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

6.7.1. 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.

6.7.2. 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.

6.7.3. 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:

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

6.7.3.2. Apresentação das funcionalidades disponibilizadas e dos recursos implementados;

6.7.3.3. Operação e utilização das funcionalidades da solução;

6.7.3.4. Procedimentos de administração e gerenciamento do ambiente;

6.7.3.5. Configuração e parametrização dos componentes da solução;

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

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

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

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

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

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

6.7.4. 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.

6.7.5. 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.

6.7.6. 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.

6.7.6.1. 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.

6.7.6.2. 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.

6.7.7. 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.

6.7.7.1. 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.

6.7.8. 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.

6.7.9. 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.

6.7.10. 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.

6.7.11. 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.

6.7.12. 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.

6.7.13. 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.

6.7.14. 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.

6.8. Requisitos de Proteção de Dados

6.8.1 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.

6.8.2. 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.

6.8.3. 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.

6.8.4 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.

6.9. Requisitos de Garantia

6.9.1. 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.

6.9.2. 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;

6.9.3. 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.

6.10. Requisitos da Exigência de amostra e ou prospecto

6.10.1. A exigência de amostra é uma prática comum em processos licitatórios e contratos administrativos, na qual os licitantes são solicitados a fornecer amostras dos produtos ou serviços que pretendem fornecer.

6.10.2. Isso permite que a administração pública avalie a qualidade, características e conformidade dos bens ou serviços propostos antes de tomar uma decisão de contratação.

6.10.3. Deverá ser analisado a necessidade de amostra a depender da solução escolhida para o melhor atendimento das necessidade.

6.10.4. A substituição de amostra por prospecto é uma prática que pode ocorrer em alguns processos licitatórios e contratos administrativos, especialmente quando se trata de bens ou serviços que não podem ser facilmente apresentados em forma física ou amostral, mas que podem ser descritos detalhadamente em um prospecto ou catálogo.

6.10.5 Assim, a substituição de amostra por prospecto pode ser uma prática adotada desde que esteja em conformidade com os princípios estabelecidos na lei e desde que seja previamente autorizada pelo edital do processo licitatório. É importante que o prospecto contenha informações detalhadas e precisas sobre as características, especificações técnicas e demais aspectos relevantes dos bens ou serviços ofertados, permitindo uma avaliação adequada por parte da administração pública.

6.10.6. Assim, a utilização de amostras, prospectos, catálogos técnicos, datasheets, demonstrações ou provas de conceito poderá ser prevista no Termo de Referência, desde que considerada necessária para a adequada avaliação do atendimento dos requisitos técnicos da solução pretendida, em conformidade com a legislação aplicável e com os princípios da Administração Pública.

6.10.7 Os critérios, condições, prazos e forma de apresentação da documentação ou das demonstrações eventualmente exigidas serão definidos oportunamente no Termo de Referência e no instrumento convocatório da contratação.

6.11. Requisitos de Subcontratação

6.11.1. Não será admitida a subcontratação do objeto.

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

6.11.3. 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.

7.LEVANTAMENTO DE MERCADO

7.1. O levantamento de mercado consiste na análise das possíveis alternativas existentes e deve abranger os aspectos técnicos e econômicos das soluções para a demanda apontada e pode ser subsidiada por diferentes fontes, para que se tenha um levantamento de mercado amplo e diverso.

7.2. Durante a pesquisa realizada no mercado de soluções voltadas ao atendimento das necessidades da instituição, não foram identificados serviços capazes de substituir a tecnologia de firewall. No entanto, os diferentes tipos de tecnologia disponíveis exigem uma análise criteriosa para identificar aquela que melhor se adequa às demandas institucionais, considerando tanto os requisitos técnicos quanto os custos envolvidos.

7.3.Dito isto, para a proposta de contratação tem-se os seguintes meios disponíveis:

7.3.1.Next Generation Firewall (NGFW);

7.3.2. Unified Threat Management (UTM).

7.4. Solução 01 – Os firewalls de próxima geração (NGFW) integram funcionalidades avançadas de segurança em uma única solução. Além do controle tradicional de pacotes de rede, possuem inspeção profunda de pacotes (DPI), filtragem de aplicações e mecanismos de detecção de ameaças. Suas principais funcionalidades incluem o controle de aplicativos, permitindo ou bloqueando softwares específicos conforme as políticas de segurança; proteção contra ameaças avançadas, como malware e ransomware; um Sistema de Prevenção de Intrusão (IPS) embutido, que analisa o tráfego e bloqueia ameaças; e visibilidade de usuários com análise em tempo real de riscos. Essa tecnologia é ideal para organizações que necessitam de um alto nível de segurança e enfrentam ameaças sofisticadas, como ataques de phishing , DDoS e malwares avançados. Sua principal vantagem é oferecer uma camada de proteção mais robusta, permitindo um controle detalhado do tráfego com base em identidades de usuários e dispositivos.

7.4.1. Pesquisa de Pregões que tem o mesmo objeto.

	Objeto	Contexto / [Item]
Pregão: 90164/2025 UASG: 250110 Nº Lei 14.133/2021	**Objeto:** Objeto: Pregão Eletrônico - Contratação de solução de tecnologia da informação e comunicação - TIC, tendo por objeto a solução de **firewall** multifuncional, do tipo Next Generation **Firewall** (NGFW), de alta capacidade para segurança de datacenter, incluindo softwares e garantia de atualização contínua, gerenciamento centralizado, serviços de instalação, configuração, implementação, suporte técnico e repasse de conhecimento, e solução de **firewall** em nuvem, para atender o Ministério da Saúde.	**FIREWALL [1]** **FIREWALL [2]**
Histórico de eventos publicados...		
Itens e Download Edital		

Fonte : https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=250110059016420 25

7.5. Solução 02 - O UTM é uma solução de segurança unificada que combina diversas funcionalidades de proteção em uma única plataforma, como firewall, VPN, IPS, antivírus e filtragem de conteúdo. Projetado como uma solução "tudo em um", oferece firewall básico e recursos avançados, como VPN e filtragem de aplicações, além de filtros de conteúdo e antimalware para bloquear ameaças externas. Também pode incluir sistemas de prevenção (IPS) e detecção de intrusão (IDS). É recomendado para pequenas e médias organizações que precisam de uma solução acessível e fácil de gerenciar, eliminando a necessidade de múltiplas ferramentas separadas. Sua principal vantagem é a centralização da segurança, reduzindo custos e complexidade operacional, sendo ideal para empresas com menor orçamento que necessitam de proteção abrangente.

7.5.1. Pesquisa de Pregões que tem o mesmo objeto.

	Objeto	Contexto / [Item]
Pregão: 90001/2025 UASG: 925772 Nº Lei 14.133/2021	**Objeto:** Objeto: Pregão Eletrônico – Contratação de pessoa jurídica especializada na renovação de licenças de proteção de rede (software), de alta disponibilidade ativa/passiva, bem como a aquisição de novos **firewall UTM** - Central Unificada de Gerenciamento de Ameaças (hardware e software na mesma caixa), visando o atendimento das necessidades da Defensoria Pública do Estado do Rio Grande do Norte.	**Nenhum registro foi encontrado com este critério**
Histórico de eventos publicados...		
Itens e Download Edital		

Fonte : https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=925772059000120 25

	Objeto	Contexto / [Item]
Pregão: 90005/2024 UASG: 980758 Nº Lei 14.133/2021	**Objeto:** Objeto: Pregão Eletrônico - Contratação de... para acesso à rede de internet banda larga + serviços para acesso à rede de internet banda larga + **firewall UTM** Integrado + Sistema de Hots... **[1] firewall UTM** Integrado + Sistema de Hotspot para atender toda estrutura Administrativa da Prefeitura Municipal de Brejetuba e seus Órgãos.Todos os pontos a serem contratados deverão ser entregues em sua totalidade com a tecnologia de fibra óptica. Serão atendidos 49 pontos com velocidade Gigabyte (velocidade simétrica (01 GB para Downloads e 01 GB para Uploads **Firewall** por 12 meses.	
Histórico de eventos publicados...		
Itens e Download Edital		

Fonte: https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=980758059000520 24

7.6. Análise comparativa das soluções

7.6.1. O Next Generation Firewall (NGFW) é uma tecnologia de segurança de rede voltada para ambientes que demandam alto desempenho, controle granular e proteção avançada. Ele combina a inspeção de pacotes com estado (stateful inspection) com a inspeção profunda de pacotes (DPI), permitindo identificar e controlar aplicações específicas, como permitir o uso do Microsoft Teams e bloquear o YouTube. Além disso, oferece funcionalidades robustas como prevenção contra intrusões (IPS/IDS), integração com serviços de inteligência contra ameaças (Threat Intelligence), inspeção de tráfego criptografado (SSL inspection), VPN e controle por identidade de usuário. Essa solução é ideal para médias e grandes organizações com infraestrutura crítica, que necessitam de ampla visibilidade, gestão centralizada e respostas eficazes a ameaças externas.

7.6.2. Já o Unified Threat Management (UTM) é uma solução integrada que reúne múltiplas funcionalidades de segurança em um único equipamento, como firewall tradicional, antivírus, VPN, IPS, filtro web e antispam. Seu foco está na facilidade de gerenciamento, com operação simplificada por meio de painéis unificados e menor necessidade de configuração especializada. Embora o desempenho e o nível de controle não sejam tão altos quanto os de um NGFW, o UTM se destaca pelo excelente custo-benefício, sendo ideal para pequenas e médias empresas ou órgãos públicos que procuram uma solução completa e acessível, com proteção adequada e gerenciamento centralizado.

7.7. Registro de soluções consideradas inviáveis

7.7.1. Entre as opções disponíveis no mercado, foram descartadas as soluções voltadas exclusivamente para ambientes em nuvem, pois se trata de um escopo específico que não atende à necessidade atual desta instituição. Esse tipo de solução poderá ser considerado em uma futura oportunidade, dependendo da estrutura que venha a ser adotada por esta Coordenadoria de Tecnologia e Informação.

7.7.2. Dentre as opções não consideradas são :

SOLUÇÃO DE FIREWALL EM NUVEM
AWS Networdk Firewall
Azure Firewall
Palo Alto Prisma Cloud
Fortinet FortiGate (Cloud)

7.8. Análise comparativa de custos (TCO)

Para a análise comparativa do Custo Total de Propriedade (TCO), foram consideradas contratações públicas de soluções de segurança de redes, contemplando equipamentos, licenciamento, subscrições de segurança, suporte técnico, atualizações e, quando previsto, serviços de instalação e configuração. Os valores apresentados possuem caráter referencial e comparativo, tendo em vista que podem variar significativamente conforme capacidade, funcionalidades, arquitetura de alta disponibilidade, período de licenciamento e nível de suporte contratado.

7.8.1. Next Generation Firewall (NGFW)

As referências pesquisadas demonstram que soluções NGFW apresentam ampla variação de preços, de acordo com o porte e as funcionalidades contratadas.

No Pregão Eletrônico nº 90011/2024, do Departamento de Estradas de Rodagem do Distrito Federal – DER/DF, foi registrada contratação para fornecimento de equipamento de segurança da informação do tipo Firewall NGFW, com licenciamento por 48 meses e treinamento, com valor homologado de R$ 518.999,00.

Em contratação da Secretaria Municipal da Fazenda de São Paulo, foi adquirido equipamento Palo Alto PA-3410, em arquitetura de alta disponibilidade, incluindo instalação, configuração, garantia, suporte e subscrições de segurança pelo período de 36 meses, pelo valor de R$ 1.500.280,00.

Também foi identificada, na Junta Comercial do Estado do Rio de Janeiro – JUCERJA, contratação para renovação de licenciamento e suporte de solução NGFW Palo Alto, no valor total de R$ 943.475,91.

Dessa forma, considerando as contratações públicas pesquisadas, observa-se que soluções NGFW corporativas podem apresentar valores da ordem de R$ 500.000,00 a R$ 1.500.000,00, ou superiores, dependendo da capacidade, arquitetura, quantidade de equipamentos, licenciamento e serviços incorporados à solução.

Fontes:

- DER/DF – Pregão Eletrônico nº 90011/2024: contratação de firewall NGFW com licenciamento por 48 meses e treinamento, valor homologado de R$ 518.999,00.
- Prefeitura de São Paulo – Contrato SF nº 43/2024: Palo Alto PA-3410, HA, suporte, garantia e subscrições de segurança por 36 meses, no valor de R$ 1.500.280,00.
- JUCERJA – Pregão Eletrônico nº 012/2024: renovação de licenciamento e suporte de NGFW Palo Alto, no valor de R$ 943.475,91.

7.8.2. Unified Threat Management (UTM)

Para soluções UTM, também foram identificadas contratações públicas envolvendo equipamentos Fortinet, licenciamento, atualizações, suporte técnico e funcionalidades integradas de segurança.

A Câmara Legislativa do Distrito Federal – CLDF, no Pregão Eletrônico nº 24/2023, estabeleceu valor de R$ 900.520,00 por equipamento para 36 meses para licenciamento e atualização de dois equipamentos FortiGate-500E, com funcionalidades UTM, suporte do fabricante e garantia. O mesmo processo contemplou ainda suporte, assistência técnica, manutenção e garantia da solução por 36 meses, no valor de R$ 385.967,16. O valor total considerado para 36 meses foi de R$ 2.721.451,66, incluindo os demais componentes previstos na contratação.

Em contratação da Universidade Tecnológica Federal do Paraná – UTFPR, foram contratadas licenças, suporte e garantia para solução de firewall composta por equipamentos FortiGate-500E, FortiGate-300E, FortiGate-200E e FortiGate-101E, pelo valor total de R$ 847.285,00.

Também foi localizada contratação de licenças, suporte e garantia para solução de firewall FortiGate-500E, pelo período de aproximadamente 15 meses, no valor de R$ 89.264,61, demonstrando a variação dos custos conforme o escopo e o período contratado.

Assim, as referências demonstram que soluções UTM podem apresentar valores bastante distintos, principalmente em razão do número de equipamentos, período de cobertura, funcionalidades de segurança, nível de suporte e serviços agregados. Para fins comparativos, recomenda-se considerar uma faixa indicativa de R$ 150.000,00 a R$ 900.000,00 ou mais, conforme o porte e a abrangência da solução.

Fontes:

- Câmara Legislativa do Distrito Federal – Pregão Eletrônico nº 24/2023: FortiGate-500E, UTM, licenciamento, atualização, suporte e garantia por 36 meses.
- UTFPR – Contrato nº 00014/2023: licenças, suporte e garantia para soluções FortiGate, valor de R$ 847.285,00.
- UTFPR – Contrato nº 00006/2025: licenças, suporte e garantia para FortiGate-500E, valor de R$ 89.264,61.

7.8.3. Comparativo Geral

ITEM	NGFW – Next Generation Firewall	UTM – Unified Threat Management
Faixa referencial observada	R$ 500.000,00 a R$ 1.500.000,00 ou mais	R$ 150.000,00 a R$ 900.000,00 ou mais
Licenciamento/Subscrições	Conforme fabricante, capacidade e funcionalidades	Conforme fabricante, capacidade e funcionalidades
Hardware/Appliance	Equipamentos de médio porte, podendo alcançar maior capacidade	Equipamentos de médio porte, podendo alcançar maior capacidade
Suporte e atualizações	Geralmente incorporados às subscrições ou contratados separadamente	Geralmente incorporados ao pacote de segurança e suporte
TCO	Elevado, especialmente em arquiteturas HA e soluções corporativas	Geralmente inferior ao NGFW de maior porte, dependendo do escopo
Aplicabilidade	Redes de maior complexidade e necessidade de controles avançados	Ambientes que necessitam de integração de múltiplas funções de segurança
Observação	Maior capacidade de inspeção, controle e recursos avançados de segurança	Integração de diversas funcionalidades em uma única solução, buscando equilíbrio entre segurança e custo

7.8.4. A análise realizada demonstra que as soluções avaliadas apresentam características técnicas relevantes para aplicação em organizações públicas, conforme a política de segurança da Coordenadoria de Tecnologia e Informação da Defensoria Pública do Estado do Amapá. Desde 2021, a instituição utiliza equipamentos de firewall da marca WatchGuard, modelos M470, T40 e T20. No entanto, considerando a evolução das ameaças cibernéticas e a necessidade de um controle mais granular e integrado da segurança de rede, conclui-se que a substituição dessa tecnologia por uma solução baseada em Next Generation Firewall (NGFW) é a alternativa mais adequada ao cenário atual.

7.8.5.A adoção de uma nova solução tecnológica com arquitetura NGFW possibilitará à Defensoria Pública modernizar sua infraestrutura de segurança, aprimorando os mecanismos de proteção contra acessos indevidos, vazamentos de dados e ataques externos. Essa medida também permitirá maior visibilidade e controle do tráfego interno e externo da rede, elevando o padrão de governança digital e resiliência institucional.

7.9. Justificativa técnica da escolha da solução

7.9.1. Após o levantamento de mercado e a análise comparativa das alternativas tecnológicas disponíveis, verificou-se que a solução baseada em Next Generation Firewall (NGFW) apresenta o melhor alinhamento com as necessidades atuais e futuras da Defensoria Pública do Estado do Amapá.

7.9.2. Embora as soluções do tipo Unified Threat Management (UTM) ofereçam recursos relevantes de proteção e gerenciamento centralizado, sua arquitetura foi concebida para cenários com menor complexidade operacional e menor demanda por recursos avançados de segurança. Considerando a evolução constante das ameaças cibernéticas, a ampliação dos serviços digitais e a crescente necessidade de proteção dos dados institucionais, torna-se necessária a adoção de uma solução com maior capacidade de inspeção, controle e resposta a incidentes.

7.9.3. As soluções NGFW disponibilizam funcionalidades avançadas de segurança, incluindo inspeção profunda de pacotes (Deep Packet Inspection – DPI), prevenção e detecção de intrusões (IPS/IDS), controle granular de aplicações, inspeção de tráfego criptografado, inteligência contra ameaças em tempo real, segmentação de rede, controle por identidade de usuário e recursos avançados de monitoramento e auditoria.

7.9.4. A adoção da tecnologia NGFW permitirá à Defensoria Pública elevar significativamente seu nível de maturidade em segurança da informação, fortalecendo a proteção dos ativos tecnológicos, dos sistemas institucionais e dos dados pessoais tratados pela instituição, em conformidade com as diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD) e com as boas práticas de governança de Tecnologia da Informação.

7.9.5. Destaca-se que as licenças atualmente utilizadas pela instituição, vinculadas à solução WatchGuard em operação, possuem vigência limitada e expiram em outubro de 2026. Embora a contratação anterior tenha garantido a continuidade dos serviços por meio da renovação das licenças por 12 (doze) meses, a presente contratação busca uma solução de longo prazo, mais moderna, escalável e aderente às necessidades estratégicas da Defensoria Pública.

7.9.6. A contratação de solução NGFW pelo período de 60 (sessenta) meses permitirá não apenas a continuidade dos serviços de proteção perimetral, mas também a modernização da infraestrutura de segurança cibernética da instituição, proporcionando maior capacidade de prevenção, detecção e resposta a ameaças digitais.

7.9.7. Sob a ótica do custo total de propriedade (TCO), embora o investimento inicial seja superior ao de soluções tradicionais, os benefícios relacionados à redução de riscos operacionais, prevenção de incidentes de segurança, continuidade dos serviços, conformidade regulatória e aumento da eficiência operacional justificam tecnicamente a adoção da tecnologia NGFW.

7.9.8. Diante do exposto, conclui-se que a contratação de uma solução de Next Generation Firewall (NGFW), acompanhada de suporte técnico especializado, garantia, atualizações de software, assinaturas de segurança e demais serviços necessários à sua plena operação, representa a alternativa mais vantajosa e adequada para atender às necessidades institucionais da Defensoria Pública do Estado do Amapá.

8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

8.1. ESPECIFICAÇÕES TÉCNICAS

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

8.1.1.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.

8.1.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

8.1.1.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderá estar listado no site do fabricante em listas de end-of-life e end-of-sale.

8.1.1.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos.

8.1.1.5. 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.

8.1.1.6. 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.

8.1.1.7. 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.

8.1.2. FUNCIONALIDADES DE REDE E FIREWALL

8.1.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

8.1.2.2. Os dispositivos de proteção de rede devem possuir suporte a VLANs;

8.1.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

8.1.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;

8.1.2.5. Os dispositivos de proteção de rede devem suportar subinterfaces Ethernet lógicas;

8.1.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

8.1.2.7. Deve implementar Network Prefix Translation (NPT v6) ou NAT66, prevenindo problemas de roteamento assimétricos;

8.1.2.8. Deverá suportar sFlow ou NetFlow;

8.1.2.9. Deve possuir suporte à criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

8.1.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

8.1.2.11. Deve suportar o protocolo padrão da indústria VXLAN;

8.1.2.12. Deve implementar o protocolo ECMP;

8.1.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

8.1.2.14. Deve enviar logs para sistemas de monitoração externos;

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

8.1.2.16. Deve possuir mecanismos de proteção anti-spoofing;

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

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

8.1.2.19. Deve suportar OSPF graceful restart;

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

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

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

8.1.2.23. Deve suportar configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

8.1.2.24. 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;

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

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

8.1.2.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção automática de certificados válidos;

8.1.2.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXi, Cisco ACI e Kubernetes;

8.1.2.29. 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;

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

8.1.2.31. Deverá suportar controle por zonas de segurança;

8.1.2.32. Deverá suportar controles de políticas por porta e protocolo;
8.1.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
8.1.2.34. Deverá suportar Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização;
8.1.2.35. Deve suportar controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
8.1.2.36. Deve suportar controle de políticas por código de país (por exemplo: BR, US, UK, RU);
8.1.2.37. Deve suportar controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
8.1.2.38. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
8.1.2.39. 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;
8.1.2.40. Deve suportar objetos e regras IPv6;
8.1.2.41. Deve suportar objetos e regras multicast;
8.1.2.42. Deve suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários predefinidos automaticamente.

8.1.3. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

8.1.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
8.1.3.2. Deve ser possível a liberação e o bloqueio somente de aplicações, sem a necessidade de liberação de portas e protocolos;
8.1.3.3. 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;
8.1.3.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
8.1.3.5. 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;
8.1.3.6. Deve inspecionar o payload do pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo;
8.1.3.7. 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;
8.1.3.8. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
8.1.3.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;
8.1.3.10. Deve identificar o uso de táticas evasivas via comunicações criptografadas;
8.1.3.11. Deve atualizar automaticamente a base de assinaturas de aplicações;
8.1.3.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller nem nas estações dos usuários;
8.1.3.13. 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;
8.1.3.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
8.1.3.15. 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;
8.1.3.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
8.1.3.17. Deve alertar o usuário quando uma aplicação for bloqueada;
8.1.3.18. Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (Bittorrent, Emule etc.), possuindo granularidade de controle e políticas para os mesmos;
8.1.3.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat etc.), possuindo granularidade de controle e políticas para os mesmos;
8.1.3.20. 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;
8.1.3.21. Deve possibilitar a diferenciação de aplicações proxy (Psiphon, Freegate etc.), possuindo granularidade de controle e políticas para as mesmas;
8.1.3.22. 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.);
8.1.3.23. 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;
8.1.3.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações, tais como: categoria da aplicação;
8.1.3.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações.

8.1.4. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

8.1.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
8.1.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
8.1.4.3. Deve sincronizar as assinaturas de IPS, Antivírus e Anti-Spyware quando implementado em alta disponibilidade;
8.1.4.4. 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;
8.1.4.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
8.1.4.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
8.1.4.7. Deve ser possível definir exceções por IP de origem ou de destino nas regras ou assinatura por assinatura;
8.1.4.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
8.1.4.9. Deve permitir o bloqueio de vulnerabilidades;
8.1.4.10. Deve permitir o bloqueio de exploits conhecidos;
8.1.4.11. Deve incluir proteção contra ataques de negação de serviço;
8.1.4.12. Deve ser imune e capaz de impedir ataques básicos como: SYN Flood, ICMP Flood, UDP Flood, entre outros;
8.1.4.13. Deve detectar e bloquear a origem de port scans;
8.1.4.14. Deve bloquear ataques efetuados por worms conhecidos;
8.1.4.15. Deve possuir assinaturas específicas para mitigação de ataques DoS e DDoS;
8.1.4.16. Deve possuir assinaturas para bloqueio de ataques de buffer overflow;
8.1.4.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
8.1.4.18. 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;
8.1.4.19. Deve permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
8.1.4.20. Deve identificar e bloquear comunicação com botnets;
8.1.4.21. 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;
8.1.4.22. Os eventos devem identificar o país de origem da ameaça;
8.1.4.23. Deve incluir proteção contra vírus em conteúdo HTML e JavaScript, software espião (spyware) e worms;
8.1.4.24. Deve possuir proteção contra downloads involuntários, utilizando HTTP, de arquivos executáveis e maliciosos;
8.1.4.25. 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;
8.1.4.26. A solução deve ter capacidade de enviar artefatos suspeitos para execução em ambiente controlado na nuvem do fabricante;
8.1.4.27. Deve suportar a captura de pacotes (PCAP) por assinatura de IPS ou por controle de aplicação;
8.1.4.28. 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.

8.1.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

8.1.5.1. 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);
8.1.5.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
8.1.5.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
8.1.5.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio não seja solicitada novamente para navegar através da solução;
8.1.5.5. Deve suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
8.1.5.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando atraso de comunicação e validação das URLs;
8.1.5.7. Deve possuir pelo menos 70 (setenta) categorias de URLs;
8.1.5.8. Deve possuir a função de exclusão de URLs do bloqueio;
8.1.5.9. Deve permitir a customização da página de bloqueio;
8.1.5.10. Deve permitir a restrição de acesso a canais específicos do YouTube, possibilitando configurar uma lista de canais liberados ou uma lista de canais bloqueados;
8.1.5.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
8.1.5.12. 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;
8.1.5.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizada.

8.1.6. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

8.1.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;
8.1.6.2. 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;
8.1.6.3. Deve possuir integração e suporte ao Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
8.1.6.4. 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;
8.1.6.5. Deve possuir integração com RADIUS para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários;
8.1.6.6. Deve possuir integração com LDAP para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários;
8.1.6.7. 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);
8.1.6.8. 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;
8.1.6.9. Deve suportar o envio e recebimento de credenciais via RADIUS;
8.1.6.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseados em atributos do LDAP/AD.

8.1.7. FUNCIONALIDADE DE FILTRO DE DADOS

8.1.7.1. Deve permitir identificar e, opcionalmente, prevenir a transferência de vários tipos de arquivos (MS Office, PDF etc.) identificados sobre aplicações (HTTP, FTP, SMTP);
8.1.7.2. Deve suportar a identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
8.1.7.3. Deve suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
8.1.7.4. 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.

8.1.8. FUNCIONALIDADE DE GEOLOCALIZAÇÃO

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

8.1.9. FUNCIONALIDADE DE VPN

8.1.9.1. Deve suportar VPN Site-to-Site e Client-to-Site;
8.1.9.2. Deve suportar IPSec VPN;
8.1.9.3. A VPN IPSec deve suportar 3DES;
8.1.9.4. A VPN IPSec deve suportar autenticação MD5 e SHA-1;
8.1.9.5. A VPN IPSec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
8.1.9.6. A VPN IPSec deve suportar Internet Key Exchange (IKEv1 e IKEv2);
8.1.9.7. A VPN IPSec deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
8.1.9.8. A VPN IPSec deve suportar autenticação via certificado IKE PKI;
8.1.9.9. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet e SonicWall;
8.1.9.10. Deve suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
8.1.9.11. Deve permitir habilitar e desabilitar túneis de VPN IPSec a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
8.1.9.12. 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;
8.1.9.13. Deve permitir atribuição de DNS aos clientes remotos de VPN;
8.1.9.14. 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;
8.1.9.15. Deve suportar autenticação via AD/LDAP, Secure ID, certificado e base de usuários local;
8.1.9.16. Deve suportar leitura e verificação de CRL (Certificate Revocation List);
8.1.9.17. Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis VPN;
8.1.9.18. Deve permitir que a conexão com a VPN seja estabelecida após autenticação do usuário na estação;
8.1.9.19. Deve permitir que a conexão com a VPN seja estabelecida sob demanda do usuário;
8.1.9.20. Deverá manter uma conexão segura com o portal durante a sessão;
8.1.9.21. O agente de VPN Client-to-Site deve ser compatível com, pelo menos:
8.1.9.21.1. Windows 10 e superior;
8.1.9.21.2. Linux Ubuntu 22.04 e superior;
8.1.9.21.3. Linux Red Hat 9;
8.1.9.21.4. Linux CentOS 9;
8.1.9.21.5. macOS 13 e superior.

8.1.10. FUNCIONALIDADE DE QoS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

8.1.10.1. 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;
8.1.10.2. Deve suportar a criação de políticas de QoS e Traffic Shaping para:
8.1.10.2.1. Endereço de origem;
8.1.10.2.2. Endereço de destino;
8.1.10.2.3. Usuário e grupo;
8.1.10.2.4. Aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
8.1.10.2.5. Porta;
8.1.10.3. O QoS deve possibilitar a definição de tráfego com banda garantida;
8.1.10.4. O QoS deve possibilitar a definição de tráfego com banda máxima;
8.1.10.5. O QoS deve possibilitar a definição de fila de prioridade;
8.1.10.5.1. Deve suportar priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
8.1.10.5.2. Deve suportar marcação de pacotes DiffServ, inclusive por aplicação;
8.1.10.5.3. Deve suportar modificação de valores DSCP para DiffServ;
8.1.10.5.4. Deve suportar priorização de tráfego utilizando informações de ToS (Type of Service);
8.1.10.5.5. Deve disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
8.1.10.5.6. Deve suportar QoS (Traffic Shaping) em interfaces agregadas ou redundantes;
8.1.10.5.7. Deve possibilitar a definição de bandas distintas para download e upload.

8.1.11. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

8.1.11.1. A solução deverá prover recursos de roteamento inteligente, permitindo definir, mediante regras pré-estabelecidas, o melhor caminho para o encaminhamento do tráfego das aplicações.
8.1.11.2. A solução deverá ser capaz de agregar múltiplos links WAN em uma interface virtual única.
8.1.11.3. 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.
8.1.11.4. 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.
8.1.11.5. A solução deverá permitir a atualização manual ou automática das políticas de balanceamento em situações de alteração da largura de banda disponível nos links.
8.1.11.6. 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).
8.1.11.7. 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).
8.1.11.8. 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:
8.1.11.8.1. Manual: deverá permitir a atribuição manual de prioridades às interfaces.
8.1.11.8.2. 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.
8.1.11.8.3. Menor Custo: deverá permitir a priorização das interfaces com base no custo previamente atribuído, desde que atendidos os requisitos mínimos de qualidade do link.
8.1.11.8.4. Balanceamento de Carga: deverá permitir a distribuição do tráfego entre todas as interfaces disponíveis, considerando algoritmos de balanceamento e os parâmetros de qualidade configurados.
8.1.11.9. A solução deverá suportar marcação de pacotes DSCP nas políticas e regras de balanceamento de tráfego.
8.1.11.10. A solução deverá suportar protocolos de roteamento dinâmico OSPFv2, OSPFv3, BGPv4 e BGP4+.
8.1.11.11. 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.
8.1.11.12. A solução deverá possibilitar a agregação de túneis IPsec, realizando balanceamento de tráfego por pacote entre os túneis configurados.

8.1.11.13. 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.
8.1.11.14. 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.
8.1.11.15. A solução deverá possuir mecanismo de correção antecipada de erros (FEC – Forward Error Correction), mediante envio de informações redundantes através de túnels VPN para compensar eventuais perdas de pacotes durante a transmissão.
8.1.11.16. 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.
8.1.11.17. A solução deverá suportar, nativamente, conectores para integração com provedores de nuvem pública.
8.1.11.18. A solução deverá permitir a configuração independente das larguras de banda de download e upload em cada interface.
8.1.11.19. 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.
8.1.11.20. A solução deverá implementar balanceamento de links utilizando algoritmo baseado em hash do endereço IP de origem.
8.1.11.21. A solução deverá implementar balanceamento de links utilizando algoritmo baseado em hash dos endereços IP de origem e destino.
8.1.11.22. 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.
8.1.11.23. 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.
8.1.11.24. 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.

8.2. 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

8.2.1.. 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.
8.2.2.. A solução deverá suportar, no mínimo, 15.000.000 (quinze milhões) de conexões simultâneas.
8.2.3.. A solução deverá suportar, no mínimo, 685.000 (seiscentas e oitenta e cinco mil) novas conexões por segundo.
8.2.4.. A solução deverá suportar throughput mínimo de 50 Gbps (cinquenta gigabits por segundo) para VPN IPsec.
8.2.5. 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.
8.2.6.. 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.
8.2.7. 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).
8.2.8. A solução deverá suportar throughput mínimo de 13,5 Gbps (treze vírgula cinco gigabits por segundo) para inspeção de tráfego SSL/TLS.
8.2.9. 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.
8.2.10. A solução deverá possuir, no mínimo, 06 (seis) interfaces MultiGigabit Ethernet 5GBase-T com conectores RJ-45.
8.2.11. A solução deverá possuir, no mínimo, 12 (doze) interfaces Gigabit Ethernet SFP.
8.2.12. A solução deverá possuir, no mínimo, 04 (quatro) interfaces 10 Gigabit Ethernet SFP+.
8.2.13. A solução deverá possuir, no mínimo, 04 (quatro) interfaces 25 Gigabit Ethernet SFP28.
8.2.14. Deverão ser fornecidos, juntamente com cada appliance NGFW, 04 (quatro) transceptores ópticos SFP+ 10GBase-SR, do mesmo fabricante da solução ofertada.
8.2.15. Deverão ser fornecidos, juntamente com cada appliance NGFW, 02 (dois) transceptores ópticos SFP28 25GBase-SR, do mesmo fabricante da solução ofertada.
8.2.16. A solução deverá possuir fontes de alimentação redundantes em corrente alternada (AC), instaladas e operacionais.
8.2.17. 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.

8.3. 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

8.3.1. 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.
8.3.2. A solução deverá suportar, no mínimo, 10.000.000 (dez milhões) de conexões simultâneas.
8.3.3. A solução deverá suportar, no mínimo, 390.000 (trezentas e noventa mil) novas conexões por segundo.
8.3.4. A solução deverá suportar throughput mínimo de 35 Gbps (trinta e cinco gigabits por segundo) para VPN IPsec.
8.3.5. 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.
8.3.6. A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 15.000 (quinze mil) túneis simultâneos de clientes VPN IPsec.
8.3.7. A solução deverá suportar throughput mínimo de 8 Gbps (oito gigabits por segundo) para a funcionalidade de Sistema de Prevenção de Intrusões (IPS).
8.3.8. A solução deverá suportar throughput mínimo de 6 Gbps (seis gigabits por segundo) para inspeção de tráfego SSL/TLS.
8.3.9. 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.
8.3.10. A solução deverá possuir, no mínimo, 08 (oito) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45.
8.3.11. A solução deverá possuir, no mínimo, 04 (quatro) interfaces Gigabit Ethernet SFP.
8.3.12. A solução deverá possuir, no mínimo, 06 (seis) interfaces 10 Gigabit Ethernet SFP+.
8.3.13. Deverão ser fornecidos, juntamente com cada appliance NGFW, 04 (quatro) transceptores ópticos SFP+ 10GBase-SR, do mesmo fabricante da solução ofertada.
8.3.14. A solução deverá possuir fontes de alimentação redundantes em corrente alternada (AC), instaladas e operacionais.
8.3.15. 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.

8.4. 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

8.4.1. 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.
8.4.2. A solução deverá suportar, no mínimo, 2.800.000 (dois milhões e oitocentas mil) conexões simultâneas.
8.4.3. A solução deverá suportar, no mínimo, 138.000 (cento e trinta e oito mil) novas conexões por segundo.
8.4.4. A solução deverá suportar throughput mínimo de 33 Gbps (trinta e três gigabits por segundo) para VPN IPsec.
8.4.5. 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.
8.4.6. A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 15.000 (quinze mil) túneis simultâneos de clientes VPN IPsec.
8.4.7. A solução deverá suportar throughput mínimo de 5 Gbps (cinco gigabits por segundo) para a funcionalidade de Sistema de Prevenção de Intrusões (IPS).
8.4.8. A solução deverá suportar throughput mínimo de 2,8 Gbps (dois vírgula oito gigabits por segundo) para inspeção de tráfego SSL/TLS.
8.4.9. 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.
8.4.10. A solução deverá possuir, no mínimo, 12 (doze) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45.
8.4.11. A solução deverá possuir, no mínimo, 08 (oito) interfaces Gigabit Ethernet SFP.
8.4.12. A solução deverá possuir, no mínimo, 04 (quatro) interfaces 10 Gigabit Ethernet SFP+.
8.4.13. Deverão ser fornecidos, juntamente com cada appliance NGFW, 04 (quatro) transceptores ópticos SFP+ 10GBase-SR, do mesmo fabricante da solução ofertada.
8.4.14. A solução deverá possuir fontes de alimentação redundantes em corrente alternada (AC), instaladas e operacionais.
8.4.15. 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.

8.5. 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

8.5.1.. 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.
8.5.2. A solução deverá suportar, no mínimo, 2.700.000 (dois milhões e setecentas mil) conexões simultâneas.
8.5.3. A solução deverá suportar, no mínimo, 120.000 (cento e vinte mil) novas conexões por segundo.
8.5.4. A solução deverá suportar throughput mínimo de 24 Gbps (vinte e quatro gigabits por segundo) para VPN IPsec.
8.5.5. 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.
8.5.6. A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 2.000 (dois mil) túneis simultâneos de clientes VPN IPsec.
8.5.7. 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).
8.5.8. A solução deverá suportar throughput mínimo de 2,4 Gbps (dois vírgula quatro gigabits por segundo) para inspeção de tráfego SSL/TLS.
8.5.9. 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.
8.5.10. A solução deverá possuir, no mínimo, 06 (seis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45.
8.5.11. A solução deverá possuir, no mínimo, 02 (duas) interfaces MultiGigabit Ethernet 5GBase-T com conectores RJ-45.
8.5.12. 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.

8.6. 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

8.6.1. 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.
8.6.2. A solução deverá suportar, no mínimo, 1.200.000 (um milhão e duzentas mil) conexões simultâneas.
8.6.3. A solução deverá suportar, no mínimo, 90.000 (noventa mil) novas conexões por segundo.
8.6.4. A solução deverá suportar throughput mínimo de 7 Gbps (sete gigabits por segundo) para VPN IPsec.
8.6.5. 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.
8.6.6. A solução deverá estar licenciada, ou suportar sem necessidade de licenciamento adicional, no mínimo, 400 (quatrocentos) túneis simultâneos de clientes VPN IPsec.
8.6.7. 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).
8.6.8. A solução deverá suportar throughput mínimo de 1,2 Gbps (um vírgula dois gigabits por segundo) para inspeção de tráfego SSL/TLS.
8.6.9. 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.
8.6.10. A solução deverá possuir, no mínimo, 06 (seis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45.
8.6.11. 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.

8.7. 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

8.7.1.1. 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.
8.7.1.2. A implantação deverá ser realizada presencialmente por profissional certificado pelo fabricante, nas dependências da CONTRATANTE.
8.7.1.3. A solução deverá ser do mesmo fabricante das soluções especificadas nos Itens 01, 02, 03, 04, 05 e 07 deste Termo de Referência.
8.7.1.4. A solução deverá suportar acesso para gerenciamento por meio dos protocolos SSH e HTTPS.
8.7.1.5. 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.
8.7.1.6. 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.
8.7.1.7. A solução deverá possuir licenciamento perpétuo, contemplando suporte do fabricante por período mínimo de 60 (sessenta) meses.
8.7.1.8. 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.
8.7.1.9. A solução não deverá impor limitação quanto à quantidade de vCPUs suportadas.
8.7.1.10. A solução não deverá impor limitação quanto à expansão de memória RAM.
8.7.1.11. A solução virtual não deverá impor limitação de armazenamento além da capacidade disponibilizada pelos discos alocados à máquina virtual.
8.7.1.12. A solução deverá permitir acesso simultâneo de administradores e possibilitar a criação de, no mínimo, 02 (dois) perfis distintos para administração e monitoramento.
8.7.1.13. A solução deverá suportar os protocolos SNMP versões 2 e 3.
8.7.1.14. A solução deverá permitir a virtualização do gerenciamento dos dispositivos, garantindo que cada administrador tenha acesso apenas aos equipamentos sob sua responsabilidade.
8.7.1.15. A solução deverá permitir a criação de administrador global com acesso irrestrito a todas as instâncias virtualizadas da plataforma.
8.7.1.16. A solução deverá suportar perfis de acesso com permissões granulares, incluindo leitura, gravação, criação de usuários e alteração de configurações gerais.
8.7.1.17. A solução deverá suportar autenticação de usuários por LDAP, RADIUS e TACACS+.
8.7.1.18. A solução deverá suportar configuração de alta disponibilidade (HA) em arquitetura Master/Slave em camada 3.
8.7.1.19. A solução deverá permitir a geração de alertas baseados nos eventos registrados nos logs.
8.7.1.20. A solução deverá disponibilizar relatórios predefinidos.
8.7.1.21. A solução deverá permitir a importação e exportação de relatórios.
8.7.1.22. A solução deverá suportar geração de relatórios de tráfego em tempo real em formato de mapa geográfico.
8.7.1.23. A solução deverá suportar geração de relatórios de tráfego em tempo real em formato de gráfico de bolhas.
8.7.1.24. A solução deverá suportar geração de relatórios de tráfego em tempo real em formato de tabela gráfica.
8.7.1.25. A solução deverá permitir a personalização de gráficos dos relatórios, incluindo gráficos de barras, linhas e tabelas.
8.7.1.26. A solução deverá permitir a personalização da capa dos relatórios.
8.7.1.27. A solução deverá permitir a geração e envio automático de relatórios periódicos.
8.7.1.28. A solução deverá permitir a geração de relatórios nos formatos HTML, CSV, XML e PDF.
8.7.1.29. A solução deverá possuir assistente gráfico para inclusão de novos dispositivos por meio de endereço IP, usuário e senha.
8.7.1.30. A solução deverá permitir visualizar a quantidade de logs enviados por cada dispositivo monitorado.
8.7.1.31. A solução deverá possuir mecanismos automáticos de remoção de logs antigos.
8.7.1.32. A solução deverá disponibilizar recurso de pesquisa detalhada (Drill-Down) para navegação em relatórios em tempo real.
8.7.1.33. A solução deverá permitir a personalização de relatórios predefinidos pelo administrador.
8.7.1.34. A solução deverá permitir o envio automático de relatórios por correio eletrônico.
8.7.1.35. A solução deverá permitir o envio de relatórios para destinatários específicos.
8.7.1.36. A solução deverá permitir o agendamento da geração de relatórios conforme calendário definido pelo administrador.
8.7.1.37. A solução deverá permitir a visualização gráfica e em tempo real da taxa de geração de logs de cada dispositivo gerenciado.
8.7.1.38. A solução deverá permitir a aplicação de filtros nos relatórios.
8.7.1.39. A solução deverá permitir a customização completa do layout dos relatórios, incluindo gráficos, textos, imagens, alinhamentos, fontes, cores e quebras de página.
8.7.1.40. A solução deverá permitir a definição do idioma dos relatórios gerados.
8.7.1.41. A solução deverá gerar alertas automáticos via e-mail, SNMP e Syslog com base em eventos, severidade e critérios definidos pelo administrador.
8.7.1.42. A solução deverá permitir o envio automático de relatórios para servidores externos via SFTP ou FTP.
8.7.1.43. A solução deverá permitir o envio automático dos logs para servidores FTP externos.
8.7.1.44. A solução deverá permitir a exportação de logs em formato CSV.
8.7.1.45. A solução deverá permitir o download dos arquivos de log para utilização externa.
8.7.1.46. A solução deverá gerar logs de auditoria contendo detalhes das alterações realizadas, identificação do administrador responsável e registro de data e hora.
8.7.1.47. Os logs dos dispositivos gerenciados deverão ser centralizados na plataforma, devendo a solução também permitir integração com servidores Syslog externos ou tecnologias equivalentes.
8.7.1.48. A solução deverá permitir a criação de consultas SQL ou tecnologia equivalente nos bancos de dados de logs para utilização em gráficos e relatórios.
8.7.1.49. 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.
8.7.1.50. A solução deverá fornecer informações sobre quantidade de logs armazenados e estimativa de retenção disponível.
8.7.1.51. A solução deverá permitir a definição de políticas de senha para administradores, incluindo tamanho mínimo e requisitos de complexidade.
8.7.1.52. A solução deverá permitir a visualização em tempo real dos logs recebidos.
8.7.1.53. A solução deverá suportar encaminhamento de logs nos formatos Syslog e CEF (Common Event Format).
8.7.1.54. A solução deverá permitir a visualização centralizada dos logs provenientes de um ou mais dispositivos, incluindo mecanismos de filtragem para facilitar pesquisas.
8.7.1.55. Os logs de auditoria e alterações de configuração deverão ser exibidos separadamente dos logs de tráfego de rede.
8.7.1.56. A solução deverá possuir painel operacional para monitoramento das principais ameaças de segurança da rede.
8.7.1.57. A solução deverá possuir painel operacional para monitoramento do comportamento dos usuários e identificação de utilização suspeita da web.
8.7.1.58. A solução deverá possuir painel operacional para monitoramento do tráfego de rede, aplicações e navegação web.
8.7.1.59. A solução deverá possuir painel operacional para monitoramento da atividade de VPN.
8.7.1.60. A solução deverá possuir painel operacional para monitoramento dos recursos locais da plataforma, incluindo CPU e memória.
8.7.1.61. A solução deverá permitir a criação de painéis personalizados para monitoramento de operações de rede e segurança.
8.7.1.62. A solução deverá disponibilizar relatórios de utilização de aplicações e mídias sociais.
8.7.1.63. A solução deverá disponibilizar relatórios de prevenção contra perda de dados (DLP).
8.7.1.64. A solução deverá disponibilizar relatórios de VPN, IPS e análise de ameaças cibernéticas.
8.7.1.65. A solução deverá disponibilizar relatório resumido diário de eventos e incidentes de segurança.
8.7.1.66. A solução deverá disponibilizar relatório de tráfego DNS e correio eletrônico.
8.7.1.67. A solução deverá disponibilizar relatório das 10 (dez) aplicações mais utilizadas na rede.
8.7.1.68. A solução deverá disponibilizar relatório dos 10 (dez) principais sites acessados na rede.
8.7.1.69. 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.
8.7.1.70. A solução deverá permitir, por meio da análise de tráfego IP, URLs e domínios acessados, identificar equipamentos potencialmente comprometidos ou usuários com comportamento suspeito.
8.7.1.71. 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.
8.7.1.72. A solução deverá permitir análise detalhada de dispositivos comprometidos, apresentando informações completas sobre as ameaças identificadas.

8.7.1.73. 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.

8.7.1.74. A solução deverá suportar correlação de eventos, disponibilizando painéis analíticos e permitindo a criação de novas visualizações para recursos de rede e segurança.

8.7.1.75. A solução deverá suportar recebimento de, no mínimo, 25 GB (vinte e cinco gigabytes) de logs por dia.

8.7.1.76. A solução deverá suportar integralmente a capacidade diária de armazenamento e processamento de logs especificada neste item, sem degradação de desempenho.

8.8. 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

8.8.1. CARACTERÍSTICAS PARA GERENCIAMENTO CENTRALIZADO

8.8.1.1. 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.

8.8.1.2. A solução deverá ser do mesmo fabricante das soluções especificadas nos Itens 01, 02, 03, 04, 05 e 06 deste Termo de Referência.

8.8.1.3. A solução deverá possuir licenciamento perpétuo, contemplando suporte do fabricante por período mínimo de 60 (sessenta) meses.

8.8.1.4. A implantação deverá ser realizada presencialmente por profissional certificado pelo fabricante, nas dependências da CONTRATANTE.

8.8.1.5. 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.

8.8.1.6. 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.

8.8.1.7. 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.

8.8.1.8. 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.

8.8.1.9. A solução não deverá impor limitação quanto à quantidade de vCPUs suportadas.

8.8.1.10. A solução não deverá impor limitação quanto à expansão de memória RAM.

8.8.1.11. 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).

8.8.1.12. 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.

8.8.1.13. 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.

8.8.1.14. A solução deverá permitir a criação de templates de configuração contendo parâmetros de DNS, SNMP, logs e administração dos dispositivos.

8.8.1.15. A solução deverá suportar arquitetura multi-tenant, permitindo o gerenciamento de ambientes independentes por meio de uma única plataforma.

8.8.1.16. A solução deverá disponibilizar APIs RESTful para integração com portais personalizados e automação da configuração de objetos e políticas de segurança.

8.8.1.17. A solução deverá garantir a integridade das configurações mediante mecanismo de bloqueio de alterações quando houver acesso simultâneo de múltiplos administradores ao mesmo ativo.

8.8.1.18. A solução deverá permitir acesso concorrente de administradores e possibilitar a definição de fluxo de aprovação para alterações realizadas.

8.8.1.19. A solução deverá permitir a criação de perfis de acesso com permissões granulares, incluindo leitura, escrita, criação de usuários e alteração de configurações.

8.8.1.20. A solução deverá permitir a utilização de palavras-chave, etiquetas ou cores para facilitar a identificação de regras.

8.8.1.21. A solução deverá permitir localizar todas as regras em que determinado objeto esteja sendo utilizado.

8.8.1.22. A solução deverá atribuir numeração sequencial às regras de Firewall, NAT e QoS.

8.8.1.23. A solução deverá permitir a criação de regras com vigência condicionada a horários específicos.

8.8.1.24. A solução deverá permitir a criação de regras com data de expiração definida.

8.8.1.25. A solução deverá realizar cópias de segurança das configurações, permitindo a restauração de versões previamente armazenadas.

8.8.1.26. 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.

8.8.1.27. A solução deverá gerar alertas automáticos por e-mail, SNMP e Syslog.

8.8.1.28. A solução deverá permitir a transferência de backups para servidores FTP, SCP ou SFTP.

8.8.1.29. A solução deverá permitir a realização de backup e rollback das configurações para versões anteriormente salvas.

8.8.1.30. A solução deverá possibilitar a visualização e comparação entre configurações atuais e versões anteriores.

8.8.1.31. A solução deverá possuir mecanismo completo de backup e restauração de suas configurações, permitindo também o agendamento automático dos processos de backup.

8.8.1.32. A solução deverá suportar a distribuição e instalação remota e centralizada de novas versões de software dos equipamentos gerenciados.

8.8.1.33. A solução deverá permitir a criação centralizada de objetos utilizados nas políticas de segurança.

8.8.1.34. A solução deverá suportar autenticação de administradores por base local e por serviços externos utilizando RADIUS, LDAP, TACACS+ e infraestrutura de chaves públicas (PKI).

8.8.1.35. A solução deverá incluir ferramenta para gerenciamento centralizado das licenças de todos os appliances administrados, permitindo a atualização das licenças diretamente pela plataforma.

8.8.1.36. A solução deverá possibilitar a distribuição e instalação remota, centralizada e automatizada de novas versões de software dos appliances gerenciados.

8.8.1.37. A solução deverá suportar o gerenciamento centralizado de pontos de acesso sem fio (Access Points).

8.8.1.38. A solução deverá suportar o gerenciamento centralizado de switches.

8.8.1.39. A solução deverá contemplar garantia, suporte técnico e direito a atualizações de software durante toda a vigência contratual de 60 (sessenta) meses.

8.9. ITEM 8 - UNIDADES DE SERVIÇOS TÉCNICOS – USTs

8.9.1. 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.

8.9.2. 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.

8.9.3. 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.

8.9.4. 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.

8.9.5. 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.

8.9.6. 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.

8.9.7. 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.

8.9.8. 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.

8.9.9. A execução dos serviços poderá ocorrer de forma presencial, remota ou híbrida, conforme a natureza da demanda e a necessidade da CONTRATANTE.

8.9.10. 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.

8.9.11. 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.

8.9.12. 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.

8.9.13. 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.

8.9.14. 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.

8.9.15. CATÁLOGO DE SERVIÇOS DE REFERÊNCIA

8.9.15.1. 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.

8.9.15.2. 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.

8.9.15.3. 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	8
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
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	16
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

8.9.15.4. 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.

8.9.15.5. 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.

8.9.15.6. 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.

8.9.15.7. 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.

8.9.15.8. A aprovação prevista no subitem anterior deverá ser formalizada pela CONTRATANTE, não sendo devido qualquer pagamento por serviço executado sem prévia autorização.

8.9.16. DA URGÊNCIA E PRIORIZAÇÃO

8.9.16.1. As demandas poderão ser classificadas pela CONTRATANTE, conforme sua criticidade, nos níveis de prioridade Alta, Média ou Baixa.

8.9.16.2. 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.

8.9.16.3. 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.

8.9.16.4. 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.

8.9.16.5. Considera-se prioridade Baixa aquela relacionada a atividades de melhoria, otimização, documentação, consultoria, ajustes não críticos ou demandas programáveis.

8.9.17. DO CONTROLE E ATESTO

8.9.17.1. 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.

8.9.17.2. 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.

8.9.17.3. 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.

8.9.17.4. 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.

8.9.17.5. As USTs previstas no contrato constituem limite máximo de consumo, não gerando direito adquirido da CONTRATADA ao seu consumo integral.

9. ESTIMATIVAS DE QUANTIDADES E VALOR A SEREM CONTRATADAS

9.1.

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/CATSER 609340).	UNIDADE	1	10	R$ 182.829,17	R$ 1.828.291,70
	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 implantação, garantia do fabricante, repasse de conhecimento e suporte, para até 10 dispositivos físicos, pelo período de 60 meses. (CATMAT/CATSER 27472).	UNIDADE	1	4	R$ 71.669,21	R$ 286.676,84
	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

9.2. A presente contratação tem por objetivo promover a modernização e a substituição da atual solução de segurança de perímetro utilizada pelo órgão, adotando um novo modelo baseado em soluções de proteção de perímetro do tipo NGFW (Next Generation Firewall), contemplando equipamentos de diferentes portes, ferramentas complementares de gestão e banco de serviços técnicos especializados.

9.3.A substituição decorre da necessidade de atualização tecnológica da infraestrutura de segurança, considerando fatores como o encerramento ou proximidade do término do ciclo de vida dos equipamentos atualmente utilizados, a evolução das ameaças cibernéticas, a necessidade de ampliação da capacidade operacional das unidades administrativas e a padronização do ambiente tecnológico institucional.

9.4.O novo modelo de contratação possibilita maior flexibilidade administrativa e técnica, permitindo que a Administração adquira equipamentos compatíveis com as demandas específicas de cada localidade, observando o crescimento da infraestrutura, a abertura de novas unidades, a substituição de ativos obsoletos e a necessidade de contingência operacional ao longo da vigência contratual.

9.5. Os quantitativos mínimos e máximos foram estabelecidos com base no levantamento da estrutura atual do órgão, na distribuição geográfica das unidades administrativas, no porte das sedes e postos descentralizados, bem como em projeções de expansão, substituição e continuidade dos serviços essenciais de tecnologia da informação.

9.6. Dessa forma, os quantitativos previstos para os itens 01 a 05 contemplam diferentes categorias de equipamentos NGFW, adequados às necessidades de processamento, throughput, número de usuários e volume de tráfego de cada unidade, permitindo que a solução seja dimensionada conforme o perfil operacional de cada sede.

9.7.O quantitativo mínimo de uma unidade para cada tipo de equipamento visa assegurar a possibilidade de atendimento imediato às necessidades identificadas durante a vigência contratual. Por sua vez, os quantitativos máximos consideram cenários de expansão institucional, substituição integral do parque tecnológico atualmente existente, implantação de redundância em unidades estratégicas e eventual criação ou reestruturação de novas sedes e unidades descentralizadas.

Item 06 – Solução de Gestão de Logs e Relatórios

9.8.A solução de gestão de logs e relatórios é indispensável para o armazenamento centralizado, retenção, correlação e análise dos eventos gerados pelos equipamentos NGFW. Sua utilização possibilita a geração de relatórios gerenciais e operacionais, apoio às atividades de auditoria, rastreabilidade das ações executadas, investigação de incidentes de segurança, atendimento a demandas dos órgãos de controle e fortalecimento da governança de segurança da informação.

9.9.O quantitativo mínimo de 01 (uma) unidade garante a operacionalização do ambiente centralizado de registros. O quantitativo máximo de 02 (duas) unidades foi definido considerando a necessidade de ampliação da capacidade de armazenamento e processamento de logs, implementação de alta disponibilidade, segregação de ambientes ou expansão do volume diário de eventos gerados pelas unidades atendidas.

Item 07 – Solução de Gestão Centralizada

9.10.A solução de gestão centralizada é necessária para administração unificada dos equipamentos NGFW, permitindo a criação e distribuição padronizada de políticas de segurança, atualização coordenada das configurações, monitoramento centralizado, gestão de objetos e regras, consolidação operacional e redução dos riscos decorrentes de configurações inconsistentes entre as unidades.

9.11.O quantitativo mínimo de 01 (uma) unidade atende ao cenário atual de gerenciamento centralizado dos ativos. O quantitativo máximo de 04 (quatro) unidades considera a possibilidade de expansão do ambiente, crescimento do número de dispositivos gerenciados, segregação por ambientes administrativos distintos, implantação de redundância e manutenção da continuidade dos serviços em situações de contingência.

Item 08 – Banco de Horas de Serviços Técnicos Especializados (USTs)

9.12.O Banco de Horas de Serviços Técnicos Especializados tem por finalidade assegurar suporte especializado sob demanda durante toda a vigência contratual, contemplando atividades que extrapolam a simples garantia dos equipamentos.

9.13. Entre os serviços passíveis de utilização destacam-se: planejamento e revisão da arquitetura de segurança; instalação e configuração avançada das soluções; migração de ambientes; atualização de versões e firmwares; otimização de desempenho; criação e revisão de políticas de segurança; implementação de novas funcionalidades; integração com serviços corporativos; apoio em auditorias; resposta e tratamento de incidentes; execução de mudanças complexas; transferência de conhecimento adicional; elaboração de documentação técnica; apoio operacional especializado e suporte consultivo para adequações decorrentes de novas necessidades institucionais.

9.14.O quantitativo mínimo de 1 (uma) hora visa garantir disponibilidade imediata para atendimentos especializados essenciais. Já o quantitativo máximo de 4.000 (quatro mil) horas foi definido considerando a possibilidade de projetos de expansão, substituições em larga escala, reconfigurações estruturais, atendimento simultâneo às diversas unidades do órgão e demandas extraordinárias que possam surgir ao longo dos 60 (sessenta) meses de vigência contratual.

9.15. Assim, os quantitativos estabelecidos refletem critérios técnicos, operacionais e prospectivos, assegurando economicidade, flexibilidade contratual e capacidade de atendimento às necessidades atuais e futuras da Administração, sem comprometer a continuidade e a efetividade dos serviços de segurança da informação.

9.16 DA UTILIZAÇÃO DO SISTEMA DE REGISTRO DE PREÇOS

9.16.1. 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.

9.16.2. A contratação pretendida contempla soluções de proteção de perímetro do tipo NGFW (Next Generation Firewall), ferramentas de gestão centralizada, soluções de armazenamento e análise de logs e relatórios, bem como banco de serviços técnicos especializados, compondo um ecossistema de segurança da informação essencial à continuidade das atividades institucionais. Trata-se de objetos cuja demanda, embora previsível em termos gerais, cuja implementação ocorrerá de forma gradual ao longo da vigência da Ata de Registro de Preços, em conformidade com a evolução das necessidades institucionais, a substituição programada de equipamentos, a expansão da infraestrutura tecnológica e a disponibilidade orçamentária da Administração.

9.16.3. A utilização do SRP mostra-se especialmente adequada diante da diversidade de perfis das unidades administrativas da Instituição, que possuem necessidades distintas de capacidade de processamento, throughput, quantidade de usuários e volume de tráfego de rede. Dessa forma, a Administração poderá realizar contratações graduais e sob demanda dos diferentes tipos de equipamentos previstos, adequando a solução às características específicas de cada sede, núcleo ou unidade descentralizada, sem a obrigatoriedade de aquisição imediata do quantitativo máximo estimado.

9.16.4. Destaca-se, ainda, que o ambiente de segurança cibernética está sujeito a constantes transformações decorrentes da evolução das ameaças digitais, da necessidade de adequação a novas exigências normativas e do crescimento dos serviços digitais ofertados pela Instituição. Nesse contexto, a adoção do Registro de Preços assegura maior capacidade de resposta da Administração diante de eventos supervenientes, permitindo a expansão do parque tecnológico, a implantação de redundância em unidades estratégicas, a substituição de ativos com falhas ou fim de vida útil e o reforço da infraestrutura de proteção sempre que necessário, observados os limites registrados em ata.

9.16.5. O modelo também se revela adequado em razão da natureza continuada dos serviços acessórios vinculados à solução. Os itens de gestão centralizada e gestão de logs constituem componentes indispensáveis para a operação integrada do ambiente de segurança, possibilitando o monitoramento unificado, a consolidação de eventos, a rastreabilidade das ações executadas, a geração de relatórios gerenciais, a investigação de incidentes e o atendimento a demandas de auditoria e órgãos de controle. A contratação sob demanda desses componentes permite que sua capacidade seja ampliada de acordo com o crescimento efetivo do ambiente protegido.

9.16.6. Da mesma forma, o Banco de Horas de Serviços Técnicos Especializados possui natureza eminentemente variável, uma vez que sua utilização está condicionada às demandas que surgirem durante a execução contratual. Poderão ser necessárias atividades de implantação, migração, atualização tecnológica, revisão de arquitetura, otimização de desempenho, resposta a incidentes, implementação de novas funcionalidades, integração com soluções corporativas, apoio consultivo e transferência adicional de conhecimento. A impossibilidade de prever com precisão o volume dessas demandas reforça a pertinência da utilização do SRP, evitando contratações insuficientes ou excessivas.

9.16.7. Sob o aspecto orçamentário, o Sistema de Registro de Preços proporciona maior racionalidade na aplicação dos recursos públicos, pois elimina a necessidade de empenho imediato sobre o quantitativo total estimado, permitindo que as aquisições sejam realizadas conforme a disponibilidade financeira e a efetiva necessidade administrativa. Tal sistemática contribui para o aprimoramento do planejamento institucional, reduz riscos de ociosidade de ativos, evita desperdícios decorrentes de superdimensionamento e assegura melhor aderência entre despesa executada e demanda real.

9.16.8. Além disso, o SRP amplia a eficiência administrativa ao reduzir a necessidade de instauração de múltiplos procedimentos licitatórios para atendimento de demandas semelhantes durante o período de vigência da ata, promovendo celeridade nas contratações, padronização tecnológica do ambiente de segurança e redução dos custos processuais associados à repetição de certames.

9.16.9. Diante do exposto, conclui-se que a adoção do Sistema de Registro de Preços para a contratação das soluções de segurança de perímetro NGFW, ferramentas de gestão, soluções de análise de logs e banco de serviços técnicos especializados constitui medida tecnicamente adequada, juridicamente amparada e economicamente vantajosa, estando alinhada aos princípios da eficiência, economicidade, planejamento, continuidade do serviço público e interesse da Administração, permitindo que a Instituição disponha de flexibilidade operacional para atender suas necessidades atuais e futuras de segurança da informação de forma segura, racional e eficiente.

9.17. DA FUNDAMENTAÇÃO DA PESQUISA DE PREÇO

9.17.1. A pesquisa de preços foi realizada com fundamento nos normativos anteriormente citados, em especial na Portaria nº 35 da DPE/AP, sendo necessária, para este processo, a adoção do parâmetro II do artigo 3º do referido ato normativo.

9.17.2. O uso do parâmetro previsto no inciso II justifica-se pela possibilidade de apuração do melhor preço estimado com base em dados de pesquisas publicadas de contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observados os índices de atualização específicos ou setoriais, admitido o Índice de Preços ao Consumidor Amplo (IPCA), se não houver outro;

9.17.3. Para a formação do valor estimado da contratação, foram realizadas pesquisas de preços no sistema Banco de preços, sendo coletadas 3 (três) referências válidas e comparáveis.

9.17.4. Os dados obtidos foram analisados quanto à sua compatibilidade com o objeto pretendido, observando-se aspectos como especificações técnicas, unidade de fornecimento e condições de execução.

9.17.5. Após a coleta e validação das informações, adotou-se como metodologia de cálculo a média aritmética simples dos valores apurados, com o objetivo de estabelecer o valor de referência da contratação, em conformidade com as práticas usuais de mercado e com os princípios da economicidade e da razoabilidade.

9.17.6.A metodologia adotada para a definição do valor de referência consiste na utilização da média aritmética simples dos preços coletados, a qual se fundamenta na soma dos valores obtidos dividida pela quantidade de referências válidas. Tal procedimento permite a obtenção de um valor representativo do mercado, reduzindo a influência de variações pontuais entre os preços pesquisados.

9.17.7. Previamente ao cálculo, os valores são analisados quanto à sua compatibilidade com o objeto da contratação, podendo ser desconsiderados aqueles que se mostrarem manifestamente inexequíveis ou excessivamente elevados. Dessa forma, a metodologia assegura maior fidedignidade à estimativa, em observância aos princípios da economicidade, razoabilidade e eficiência

9.17.8.A memória de cálculo encontra-se nos autos do processo SEI (Doc nº 0270394 e 0270396) elaborada em documento separado em razão da quantidade de informação extraída do programa utilizado para elaboração da pesquisa de preço. Sua inserção neste documento poderia causar instabilidade e dificultar a análise, devido à possível perda de qualidade das imagens e a inserção equivocada de informação.

10. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

10.1. 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.

10.2. 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.

10.3. 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.

10.4. 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.

10.5. 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.

10.6. 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.

10.7. 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.

11. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

11.1. A presente contratação será realizada de forma independente, sem a necessidade de contratações correlatas ou interdependentes.

11.2. Embora a presente contratação seja realizada de forma independente, recomenda-se, como ação complementar estratégica, o fornecimento de curso de capacitação e atualização para a equipe de Tecnologia da Informação da Defensoria Pública do Estado do Amapá, com foco específico em cibersegurança, gestão de incidentes, análise de ameaças e operação da solução de Next Generation Firewall (NGFW) a ser implantada, incluindo seus recursos avançados de prevenção de intrusões, inspeção de tráfego, controle de aplicações, inteligência contra ameaças, monitoramento e resposta a incidentes.

11.3.A referida iniciativa tem como objetivo fortalecer as competências técnicas dos servidores responsáveis pela segurança da informação, assegurando a correta administração, operação, manutenção e evolução da solução contratada, bem como a maximização dos investimentos realizados em segurança cibernética. Busca-se, ainda, promover maior autonomia operacional da equipe técnica institucional, contribuindo para o aprimoramento contínuo dos mecanismos de proteção dos ativos tecnológicos, da disponibilidade dos serviços e da proteção dos dados sob responsabilidade da Defensoria Pública, em consonância com as boas práticas de governança, segurança da informação e proteção de dados pessoais.

12. DEMONSTRAÇÃO DO ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO DA DEFENSORIA PÚBLICA DO ESTADO DO AMAPÁ

12.1. Conforme Portaria nº 33/2024 - DPE/AP, publicada em 10 de janeiro de 2024, o plano de contratações anual consolida as demandas que se planeja contratar no exercício subsequente ao de sua elaboração e, de acordo com o art. 5º daquela Portaria, até o final do mês de agosto de cada exercício, a DPE/AP deverá elaborar o seu plano de contratações anual.

12.2. A presente aquisição está prevista no PCA da Defensoria Pública, devidamente publicada no portal nacional de Contratações Públicas (https://pncp.gov.br/app/pca/11762144000100/2025), bem como no sítio oficial da DPE/AP (https://defensoria.ap.def.br/transparencias/6ºChegadaCorregedoria), em atendimento ao que prevê o art. 10, § 2º e § 3º da Portaria nº 33/2024 - DPE/AP.

12.3. Além do cumprimento legal previsto no art. 12, inciso VII, § 1º, da Lei Federal nº 14.133/2021, a instituição reforça seu planejamento estratégico, a otimização de recursos, a transparência e o fortalecimento da eficiência operacional, a fim de que os processos de compras e contratações se tornem mais ágeis e organizados, garantindo que as demandas sejam entregues no momento adequado, sem prejudicar a atividade-fim da Defensoria Pública.

13. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

13.1. Com a contratação da solução de segurança de perímetro baseada em tecnologia Next Generation Firewall (NGFW), a Defensoria Pública do Estado do Amapá pretende elevar o nível de maturidade de sua segurança cibernética, fortalecendo a proteção dos ativos tecnológicos, sistemas corporativos, serviços digitais e dados institucionais sob sua responsabilidade. O principal resultado esperado é a ampliação da capacidade de prevenção, detecção e resposta a ameaças cibernéticas cada vez mais sofisticadas, reduzindo os riscos de acessos não autorizados, vazamentos de dados, indisponibilidade de serviços e demais incidentes de segurança da informação.

13.2. A adoção da solução NGFW proporcionará maior visibilidade e controle sobre o tráfego de rede, permitindo a identificação de aplicações, usuários, dispositivos e comportamentos potencialmente maliciosos. Além disso, recursos avançados como inspeção profunda de pacotes (DPI), prevenção de intrusões (IPS), inspeção de tráfego criptografado, inteligência contra ameaças e monitoramento em tempo real contribuirão para o fortalecimento da postura de segurança institucional e para a mitigação proativa de riscos.

13.3. A solução também deverá aprimorar a governança de Tecnologia da Informação e Segurança da Informação por meio da centralização do gerenciamento, monitoramento contínuo do ambiente, geração de relatórios gerenciais, rastreabilidade de eventos e aplicação uniforme de políticas de segurança. Como consequência, espera-se maior eficiência operacional da equipe técnica, redução do tempo de resposta a incidentes e maior capacidade de planejamento e tomada de decisão baseada em informações confiáveis.

13.4. Outro resultado esperado consiste na manutenção da conformidade com as boas práticas de segurança da informação e com os requisitos legais relacionados à proteção de dados pessoais, especialmente aqueles estabelecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), contribuindo para a preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações tratadas pela instituição.

13.5. Por fim, espera-se que a solução contratada proporcione uma infraestrutura de segurança moderna, escalável e preparada para acompanhar a evolução tecnológica da Defensoria Pública do Estado do Amapá, permitindo futuras expansões de capacidade, integração com novos serviços e adequação às mudanças do cenário de ameaças cibernéticas. Dessa forma, busca-se garantir a continuidade dos serviços prestados à sociedade com elevados níveis de disponibilidade, estabilidade, desempenho e segurança.

14. PROVIDÊNCIAS A SEREM ADOTADAS

14.1. As providências adotadas serão :

14.1.1.Publicidade dos atos processuais nos termos da Lei Federal nº 14.133, de 2021.

14.1.2. Execução, recebimento e aceite do objeto dentro dos prazos estabelecidos.

14.1.3. Providências quanto ao pagamento dos serviços, conforme for habilitadas as licenças, após emissão da nota fiscal da contratada e termo de recebimento definitivo emitido por fiscal designado pela contratante.

15. POSSÍVEIS IMPACTOS AMBIENTAIS

15.1. As especificações dos itens a serem adquiridos contemplam elementos com baixa capacidade de causar danos ambientais. Além disso, as especificações estão em conformidade com as disposições relacionadas às contratações sustentáveis, dispostas no Guia Nacional Prático de Contratações Sustentáveis - 6º Ed, em que os produtos deverão ser de baixo impacto ambiental, com materiais menos agressivos ao meio ambiente, com maior eficiência na utilização dos recursos naturais e maior vida útil.

16. CONCLUSÃO QUANTO À VIABILIDADE E ADEQUAÇÃO DA CONTRATAÇÃO

16.1. Diante de toda a análise desenvolvida no presente Estudo, a contratação mostra-se viável em termos de disponibilidade de mercado, forma de fornecimento do objeto, competitividade do mercado, além de mostrar-se tecnicamente possível e fundamentadamente necessária, não se observando óbices ao prosseguimento da futura contratação.

17. CLASSIFICAÇÃO DA INFORMAÇÃO

17.1. Em atendimento ao que dispõe o art. 7º da Portaria nº 37/2024 - DPE/AP, tendo em vista o baixo grau de complexidade do objeto e o seu caráter comum, verifica-se que as informações contidas neste Estudo 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.

(Assinado Eletronicamente)
WALTER DA SILVA ARAÚJO FILHO
Coordenador de Tecnologia da Informação
Portaria nº 108, de 24 de janeiro de 2024

(Assinatura eletronicamente)
ROGÉRIO LEITE MORESCO
Assessor Técnico Nível III
Coordenadoria de Licitações, Contratos e Convênios
Portaria nº 1103, de 03 de Outubro de 2023

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 **0270324** e o código CRC **0899E318**.