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.° SEI n.º 25.0.000001155-2

1.2. Número da Contratação PCA: UASG 927560, Documento de Formalização**147/2024.**

2. OBJETO

2.1. O presente Estudo Técnico Preliminar, tem como objetivo eventual Contratação de solução de Firewall

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 (0074531) **Prosseguimento do Processo Licitatório**: Autoriza-se o prosseguimento do processo licitatório referente à **contratação n.º 08/2025 – TIC - Software e Licenças**, prevista no PCA/2025, dando-se continuidade à execução do calendário aprovado pelo Defensor Público-Geral, **ID do item** n.º **194 a 203** - *Link de acesso ao PCA/2025 (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 um papel essencial na garantia do acesso à justiça, prestando assistência jurídica à população. Como instituição pública, lida diariamente com informações sensíveis e dados sigilosos de cidadãos, processos judiciais e administrativos.

4.2. Diante disso, a segurança cibernética se torna uma prioridade estratégica, e a implementação de uma solução em firewall[1] é indispensável para garantir a proteção desses ativos críticos.

4.3. O firewall atua como uma barreira de defesa contra ameaças cibernéticas, controlando o tráfego de rede e impedindo acessos não autorizados. Sem um sistema robusto de segurança, a Defensoria Pública fica vulnerável a ataques como invasões, vazamentos de dados, sequestro de informações (ransomware[2]) e indisponibilidade dos serviços essenciais.

4.4. Além disso, considerando a crescente digitalização dos serviços públicos e a necessidade de conformidade com normas de segurança da informação, a adoção de uma solução em firewall moderna se torna fundamental para assegurar a integridade, confidencialidade e disponibilidade dos sistemas institucionais.

4.5. A Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018[3]) impõe à Administração Pública o dever de proteger os dados pessoais sob sua custódia, reforçando a necessidade de mecanismos de defesa eficazes contra acessos indevidos e vazamentos. A ausência de um firewall adequado pode resultar em responsabilidade administrativa e jurídica, além de comprometer a confiança dos cidadãos na Defensoria Pública.

4.6. Atualmente, a Defensoria Pública do Estado do Amapá dispõe de equipamentos de firewall em sua estrutura de segurança cibernética[4] . No entanto, as licenças desses dispositivos encontram-se vencidas, comprometendo a efetividade da proteção contra ameaças virtuais.

4.7. Sem as atualizações e suporte adequados, os equipamentos não conseguem oferecer a segurança necessária para a proteção dos dados institucionais, aumentando os riscos de vulnerabilidades, acessos não autorizados e possíveis incidentes de segurança.

4.8. Além da necessidade de renovação das licenças, a crescente demanda por serviços digitais e o aumento do tráfego de dados exigem um reforço na estrutura de defesa da Defensoria Pública.

4.9. O parque tecnológico atual necessita de expansão, com a aquisição de novos equipamentos que ampliem a capacidade de proteção da rede, garantindo maior disponibilidade, desempenho e segurança para os sistemas institucionais.

4.10. Diante desse cenário, torna-se essencial a contratação das licenças e a ampliação dos recursos de firewall, assegurando a continuidade dos serviços prestados com integridade e conformidade com as normativas de segurança da informação.

4.11. O presente estudo técnico preliminar irá avaliar a necessidade de contratação e identificar as melhores opções que atendam às demandas da instituição com eficiência e custo-benefício.

4.12. Destaca-se que o objeto desta contratação não se enquadra na categoria bens e serviços de luxo, conforme descrição contida no art. 4º, inciso III da Portaria nº 32/2024 - DPE/AP.

5. ÁREA REQUISITANTE

5.1.

Área requisitante	Responsável
Coordenadoria de Tecnologia e Informação	**Walter da Silva Araújo Filho**

6. REQUISITOS DA CONTRATAÇÃO

6.1. Requisitos de Negócio

6.1.1. Promover o acesso à justiça e proteger os direitos do cidadão;

6.1.2. Aperfeiçoar a coordenação estratégica e o acesso do cidadão à garantia dos seus direitos;

6.1.3. Aprimorar os meios de gestão e a governança institucional.

6.1.4. Aprimorar os mecanismos de segurança da informação, tanto dos usuários da Defensoria Pública do Estado do Amapá, quanto dos usuários externos;

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 contratada deverá manter equipe à disposição de segunda a sexta-feira, das 07:30h às 13h30, durante a execução do contrato.

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 - 6ª Edição, Setembro/2023, 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

6.5.1. A contratação de licenças de firewall UTM (Unified Threat Management) da WatchGuard[5] exige a observância de requisitos tecnológicos que garantam a plena compatibilidade com o ambiente de rede da instituição. É fundamental que as licenças contemplem os recursos de segurança avançada, como prevenção contra intrusões (IPS)[6] , controle de aplicações, antivírus de gateway, filtragem de conteúdo web e proteção contra ameaças persistentes. Esses recursos devem estar integrados à solução UTM, possibilitando a gestão unificada e centralizada de políticas de segurança, com atualização constante das bases de dados de ameaças.

6.5.2.Outro requisito essencial é que as licenças sejam compatíveis com os modelos de appliance[7] já existentes ou previstos para aquisição, respeitando a capacidade de throughput[8] recomendada para o volume de tráfego da rede. A solução contratada deve permitir a gestão em nuvem (Cloud Management)[9] e oferecer suporte a VPNs[10] seguras (IPSec[11] e SSL[12]), além de autenticação robusta de usuários e dispositivos. A escalabilidade[13] também é um critério importante, permitindo a expansão da cobertura de segurança conforme o crescimento da rede institucional, sem perda de desempenho.

6.5.3. Por fim, as licenças devem prever suporte técnico especializado, com

atualizações automáticas de firmware[14] e definições de segurança durante todo o período de vigência. É recomendável que a contratação inclua acesso ao WatchGuard Total Security Suite ou equivalente, para assegurar um pacote completo de proteção cibernética, relatórios detalhados, e integração com ferramentas de análise e resposta a incidentes. Dessa forma, garante-se não apenas a conformidade com boas práticas de segurança da informação, mas também a continuidade operacional e a mitigação de riscos cibernéticos críticos.

6.6. Requisitos de Instalação e Configuração

6.6.1. A instalação e configuração das licenças, serão realizados pelos técnicos da Defensoria Pública do Estado do Amapá;

6.6.2. Para garantir a perfeita integração da solução com o parque tecnológico do DPE/AP, e ainda, que os serviços de instalação sejam efetuados de acordo com as recomendações do fabricante, os serviços de instalação, configuração, serão realizados pelos técnicos da Defensoria Pública do Estado do Amapá com auxílio dos técnicos da contratada;

6.7. Requisitos de Proteção de Dados

6.7.1.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.

6.7.2.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.

6.7.3.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.

6.7.4.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.

6.8. Requisitos de Garantia

6.8.1. A solução deverá possuir **licenciamento pleno por 12 meses**, abrangendo todas as funcionalidades sem limitação por recurso. O fabricante deve garantir suporte e atualizações durante o período da vigência das licenças.

6.8.2. O prazo de garantia para esta contratação é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

6.9. Requisitos da Exigência de amostra e ou prospecto

6.9.1. 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.
6.9.2. Isso permite que a administração pública avalie a qualidade, características e conformidade dos bens ou serviços propostos antes de tomar uma decisão de contratação.
6.9.3.. Deverá ser analisado a necessidade de amostra a depender da solução escolhida para o melhor atendimento das necessidade.
6.9.4. 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.
6.9.5.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. Requisitos de Subcontratação

6.10.1. Não será admitida a subcontratação do objeto, conforme estatui o §4º, do art. 74, da Lei nº 14.133, de 2021.

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:

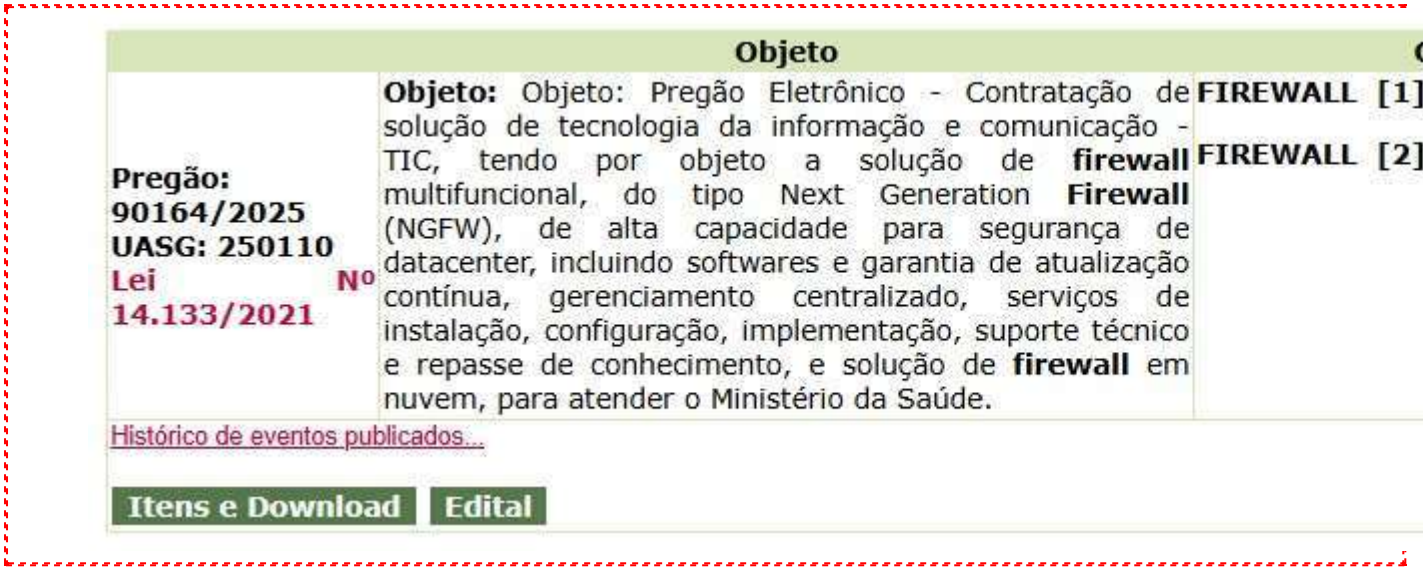
7.3.1.**Next Generation Firewall (NGFW);**

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[15] e ransomware; um Sistema de

Prevenção de Intrusão (IPS)[16] 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[17] , DDoS[18] 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		
Pregão: 90164/2025 UASG: 250110 Lei Nº 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]**

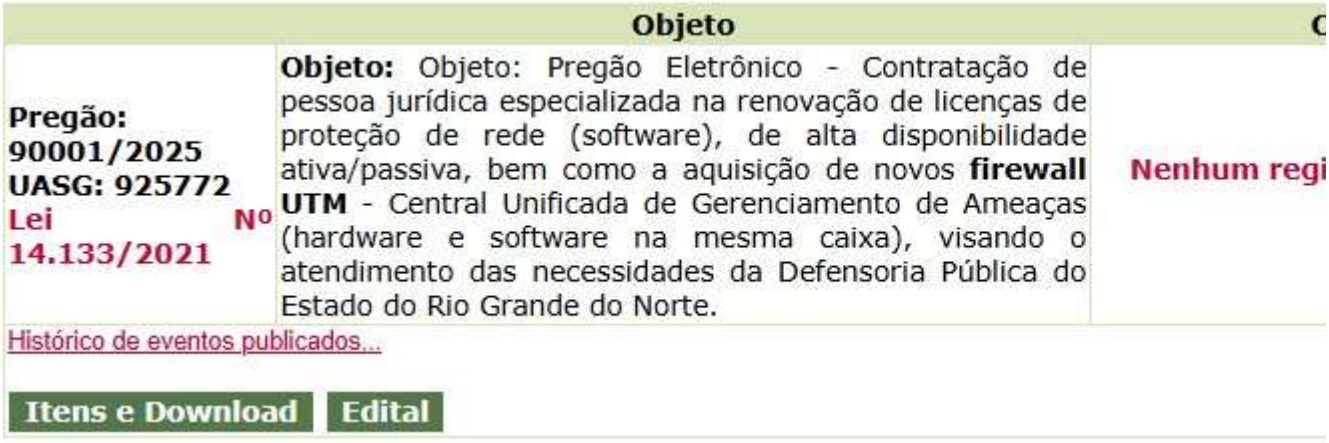
Histórico de eventos publicados...

Itens e Download | Edital

[19] **Fonte:** http://comprasnet.gov.br/ConsultaLicitacoes/

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.

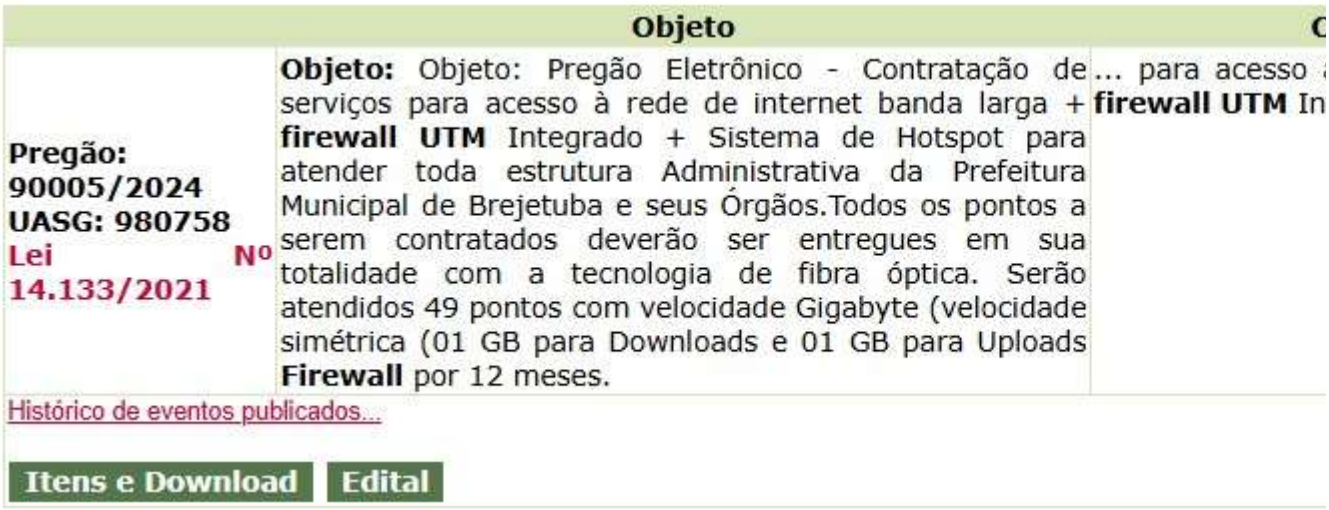
7.5.1. Pesquisa de Pregões que tem o mesmo objeto.



Objeto		
Pregão: 90001/2025 UASG: 925772 Lei Nº 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 regi

Histórico de eventos publicados...

Itens e Download | Edital



[20] **Fonte:** http://comprasnet.gov.br/ConsultaLicitacoes/

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[21]) 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[22]), inspeção de tráfego criptografado (SSL inspection[23]), 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

Solução de Firewall em Nuvem
Palo Alto Prisma Cloud
Fortinet FortiGate (Cloud)

7.8. Análise comparativa de custos (TCO)

7.8.1. Next Generation Firewall (NGFW)

- **Licenciamento:** O custo de licenciamento para NGFWs de empresas como Cisco, Fortinet ou Palo Alto pode variar entre **R$ 50.000 a R$ 150.000 por ano**, totalizando entre **R$ 250.000 a R$ 750.000 em 5 anos**, conforme funcionalidades e escalabilidade.
- **Hardware:** Equipamentos de NGFW de média capacidade têm custo entre **R$ 100.000 a R$ 200.000**.
- **Suporte e Atualizações:** Custos adicionais de suporte e atualizações variam entre **R$ 10.000 a R$ 40.000 por ano**, totalizando **R$ 50.000 a R$ 200.000 em 5 anos**
- **Custos Totais em 60 Meses:** Aproximadamente entre **R$ 400.000 a R$ 1.150.000**.
- **Observação:** Essa é a solução mais cara, justificada pela segurança avançada e escalabilidade, ideal para redes grandes e complexas.

7.8.2. Unified Threat Management (UTM)

- **Licenciamento:** O custo médio anual para licenciamento de soluções UTM varia entre **R$ 20.000 a R$ 50.000**, totalizando **R$ 100.000 a R$ 250.000 em 5 anos**
- **Hardware:** Equipamentos UTM de médio porte custam entre **R$ 60.000 a R$ 100.000**.
- **Suporte e Atualizações:** Os custos variam entre **R$ 5.000 a R$ 15.000 por ano**, somando **R$ 25.000 a R$ 75.000 em 5 anos**
- **Custos Totais em 60 Meses:** Aproximadamente entre **R$ 185.000 a R$ 425.000**.
- **Observação:** Essa solução oferece equilíbrio entre custo e funcionalidade, integrando múltiplas camadas de segurança em um único dispositivo. É ideal para organizações públicas de médio porte que buscam segurança centralizada e simplificação de gerenciamento.

7.8.3. Comparativo Geral

Item	NGFW (Next Generation Firewall)	UTM (Unified Threat Management)
Licenciamento (5 anos)	R$ 250.000 – R$ 750.000	R$ 100.000 – R$ 250.000
Hardware	R$ 100.000 – R$ 200.000	R$ 60.000 – R$ 100.000
Suporte e Atualizações	R$ 50.000 – R$ 200.000	R$ 25.000 – R$ 75.000
Custo Total (5 anos)	**R$ 400.000 – R$ 1.150.000**	**R$ 185.000 – R$ 425.000**

Item	NGFW (Next Generation Firewall)	UTM (Unified Threat Management)
Observação	Solução robusta, segura e escalável. Ideal para redes complexas.	Solução integrada e equilibrada. Ideal para redes de médio porte.

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. Apesar de o estudo técnico preliminar reconhecer que a tecnologia de *Next Generation Firewall* (NGFW) representa a solução mais moderna e robusta em segurança de rede, oferecendo funcionalidades avançadas como *Deep Packet Inspection (DPI)*[24] , controle granular de aplicações, proteção contra ameaças persistentes, e maior visibilidade do tráfego com base na identidade dos usuários, a adoção dessa arquitetura no presente momento mostra-se financeiramente inviável para a realidade da Defensoria Pública do Estado do Amapá.

7.9.2.A análise de custo total de propriedade (TCO) apresentada no ETP revela que os investimentos necessários para implantação de um NGFW podem ultrapassar R$ 1.150.000,00 em cinco anos, valor incompatível com o orçamento atual da instituição, além de demandar maior estrutura técnica para sua gestão e manutenção contínuas.

7.9.3. Considerando a barreira orçamentária que inviabiliza, neste momento, a implementação de uma solução mais avançada, optou-se por manter a atual arquitetura baseada em tecnologia UTM (Unified Threat Management). Embora tecnicamente menos robusta em comparação com soluções de última geração, a UTM integra, em uma única plataforma, os principais mecanismos de defesa — como firewall, antivírus, VPN, IPS, controle de aplicações e filtro de conteúdo — com gestão centralizada, atualizações contínuas e um custo de aquisição e manutenção significativamente mais acessível.

7.9.4. A solução UTM da marca WatchGuard, já integrada ao parque tecnológico da Defensoria Pública, tem se mostrado adequada às necessidades institucionais de segurança da informação. Dessa forma, optou-se, de forma estratégica e racional, por renovar exclusivamente as licenças vencidas dos equipamentos atualmente em uso, evitando a necessidade de aquisição de novos dispositivos. Tal decisão está plenamente alinhada ao princípio da economicidade, ao planejamento institucional vigente, às diretrizes legais e à realidade orçamentária da Administração Pública, promovendo a continuidade dos serviços com segurança, estabilidade e responsabilidade fiscal.

7.9.5. Ressalta-se, no entanto, que a adoção de uma solução mais moderna, como o Next Generation Firewall (NGFW), permanece como uma meta estratégica para o futuro, sendo essencial para fortalecer ainda mais os mecanismos de proteção cibernética da instituição diante do avanço constante das ameaças digitais. A segurança da informação deve ser tratada como área prioritária de investimento contínuo, considerando o papel essencial da Defensoria Pública na proteção de dados sensíveis dos cidadãos e na garantia da prestação de serviços com integridade, disponibilidade e confidencialidade

8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

8.1.

ITEM 1: Renovação de licença Basic Security pelo período de 12 meses para o Appliance M470:

1.1. Composição do fornecimento (2 unidades), sendo (software):

1.1.1. 1 unidades – WatchGuard Basic Security Suite Renewal/Upgrade 1-yr for M470 (WGM47331)

1.2. A licença deverá ser associada aos appliances com seriais 80100583D-20CF e 8010055EA-80B8;

1.3. A licença deverá contemplar os seguintes requisitos: controle de aplicação, filtro de conteúdo web, IPS, antispam e antivírus de gateway. Prover suporte técnico, manutenção/garantia e atualização de firmware e assinatura por 12 meses.

8.2.

ITEM 2: Renovação de licença Basic Security pelo período de 12 meses para o Appliance Watchguard T40.

2.1. Composição do fornecimento do item (software):

2.1.1. A licença deverá ser associada ao appliance com serial D0280C611-A676;

2.2. A licença deverá contemplar os seguintes requisitos: controle de aplicação, filtro de conteúdo web, IPS, antispam e antivírus de gateway. Prover suporte técnico, manutenção/garantia e atualização de firmware e assinaturas por 12 meses.

8.3.

ITEM 3: Renovação de licença Basic Security pelo período de 12 meses para o Appliance Watchguard T20.

3.1. Composição do fornecimento (10 unidades), sendo (software):

3.1.1. 1 unidades – WatchGuard Basic Security Suite Renewal/Upgrade 1-yr for Firebox T20 (WGT20341).

3.2. As licenças deverão ser associadas aos appliances com seriais:

3.2.1. D0260DC95-2561;

3.2.2. D0260DC7C-A3E4;

3.2.3. D0260DC7B-6325;

3.2.4. D0260CC5E-B564;

3.2.5. D026144AF-DA95;

3.2.6. D0260DC84-75A1;

3.2.7. D0260DCA3-27C3;

3.2.8. D0260DFBA-F353;

3.2.9. D0260DC6F-3025;

3.2.10. D0260DCC0-4682;

3.3. A licença deverá contemplar os seguintes requisitos: controle de aplicação, filtro de conteúdo web, IPS, antispam e antivírus de gateway. Prover suporte técnico, manutenção/garantia e atualização de firmware e assinaturas por 12 meses.

9. ESTIMATIVAS DE QUANTIDADES E VALOR A SEREM CONTRATADAS

9.1.

ITEM	DESCRIÇÃO	QUANTIDADE	Portal de Contratações Públicas (P Pregão Eletrônico nº 01/2025 - DPE/RN (9 Comprasnet) PNCP (https://pncp.gov.br/app/editais/076288440

01	Renovação de licença Basic Security pelo período de 12 meses para o Appliance Watchguard M470. Composição do fornecimento do item: Licenças WatchGuard Basic Security Suite Renewal/Upgrade 1-ano para M470 (WGM47331) Características técnicas: Composição do fornecimento do item (software): 1 unidade – WatchGuard Basic Security Suite Renewal/Upgrade 1-ano para M470 (WGM47331) **(CATMAT 609340)**	02	**R$ 34.000,00**

02	Renovação de licença Basic Security pelo período de 12 meses para o Appliance Watchguard T40. Composição do fornecimento do item: Licenças WatchGuard Basic Security Suite Renewal/Upgrade 1-ano para Firebox T40 (WGT40341) Características técnicas: Composição do fornecimento do item (software): 1 unidade – WatchGuard Basic Security Suite Renewal/Upgrade 1-ano para Firebox T40 (WGT40341). **(CATMAT 609340)**	01	**R$ 7.760,00**

03	Renovação de licença Basic Security pelo período de 12 meses para o Appliance Watchguard T20. Composição do fornecimento do item: Linceças WatchGuard Basic Security Suite Renewal/Upgrade 1 - ano para Firebox T20 (WGT20341) Características técnicas: Composição do fornecimento, sendo (software): 1 unidade – WatchGuard Basic Security Suite Renewal/Upgrade 1- ano para Firebox T20 (WGT20341). **(CATSER 609340)**	10	**R$ 4.650,00**
			TOTAL

9.2. A definição do quantitativo considerou a estrutura física e lógica das unidades da Defensoria Pública do Estado do Amapá, bem como as particularidades operacionais de cada localidade. Para o **Item 01**, referente à renovação da licença **WatchGuard Basic Security Suite Renewal/Upgrade 1 ano para o appliance M470 (WGM47331)**, contempla a unidade **sede** da Defensoria Pública e **dois anexos localizados no município de Macapá**, onde há maior demanda de tráfego de dados e serviços interligados em rede. Trata-se de um equipamento de maior capacidade, cuja renovação da licença é essencial para garantir o funcionamento dos serviços centrais de segurança, filtragem de conteúdo, antivírus, controle de aplicações e demais funcionalidades integradas à suíte básica de segurança.

9.3.Já o o **Item 02**, correspondente à licença **WatchGuard Basic Security Suite Renewal/Upgrade 1 ano para o appliance Firebox T40 (WGT40341)**, destina-se ao atendimento de outra estrutura da Defensoria também localizada no **município de Santana**, responsável por demandas setoriais específicas. O appliance T40 possui capacidade técnica adequada para o volume de usuários da unidade e sua renovação é imprescindível para manter os níveis de proteção exigidos pelas normas de segurança da informação.

9.4. Por fim, o **Item 03**, que trata da renovação da licença **WatchGuard Basic Security Suite Renewal/Upgrade 1 ano para o appliance Firebox T20 (WGT20341)**, refere-se aos equipamentos instalados nas **unidades da Defensoria situadas em outros municípios do interior do Estado do Amapá**. Cada unidade conta com um appliance T20 dedicado, compatível com o porte da rede local e com as demandas de segurança regionais. A

renovação garante a continuidade da proteção descentralizada dos dados institucionais e o cumprimento dos padrões mínimos de cibersegurança exigidos para o setor público.

9.5. A utilização do **Sistema de Registro de Preços** para esta contratação apresenta grande relevância, uma vez que possibilita a aquisição futura de licenças adicionais ou renovações de forma ágil e com preços previamente estabelecidos, garantindo eficiência, economicidade e planejamento orçamentário. A criação da **Ata de Registro de Preços** formaliza os compromissos entre a Administração e os fornecedores, permitindo que a Defensoria Pública realize aquisições conforme a necessidade das unidades, sem a necessidade de novos processos licitatórios para cada demanda. Este instrumento também assegura transparência, padronização e segurança jurídica em todo o processo de contratação.

9.6.DA PESQUISA DE PREÇO

9.6.1.A presente pesquisa se baseou no Art. 23 da Lei nº 14.133/21; Art. 5º da Instrução Normativa SEGES/ME, nº 65 e art. 3º da Portaria nº 35 da DPE/AP.

9.6.2..A pesquisa de preços foi realizada com base nos normativos anteriormente citados, sendo necessária, para este processo, a combinação de vários parâmetros, correspondentes aos itens II[25] , III[26] e IV[27] .

9.6.3. A pesquisa de preços iniciou-se pela coleta de cotações no Portal Nacional de Contratações Públicas (PNCP), utilizando-se o parâmetro II. Contudo, obteve-se apenas uma cotação compatível com as características do objeto. Diante disso, aplicou-se o parâmetro IV, realizando consultas de preços por meio de correio eletrônico a empresas que já haviam participado de outras licitações com objeto semelhante. No total, foram consultadas 11 (onze) empresas, sendo que apenas uma respondeu com a cotação, três (03) manifestaram não ter interesse, e não houve retorno das demais, resultando em êxito com apenas uma empresa. Em seguida, com base no parâmetro III, foi necessária a realização de pesquisa de preços em âmbito mais amplo, dada a dificuldade de obtenção de valores. Para tanto, foram consultados três (03) sites estrangeiros, com o objetivo de identificar um preço de referência plausível para compor o cálculo, cuja memória encontra-se em anexo (SEI 0138076), sendo realizado a conversão do valor em dólar para o real e a aplicação de impostos incidente ao tipo do objeto.

9.6.4. Após a composição de três (3) preços (PNCP (0138074), Fornecedor Direto (0138075) e Domínio Amplo (0136271)), aplicou-se a metodologia da média aritmética simples, de forma a identificar o valor estimado da contratação, como mostra a tabela do Item 9.1.

9.6.5. A adoção combinada dos parâmetros mostrou-se essencial para a realização de uma estimativa de preços mais próxima da realidade, com o objetivo de fornecer uma cotação precisa, transparente, confiável e de acordo com os valores praticados no mercado.

10. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

10.1.A contratação da solução de segurança de perímetro com tecnologia UTM (Unified Threat Management) deve ser realizada por lote único, considerando que a arquitetura proposta integra, em uma única plataforma, diversas camadas de proteção — como firewall, antivírus, filtro de conteúdo, VPN, controle de aplicações e prevenção contra intrusões. A separação dos itens entre diferentes fornecedores comprometeria a padronização e a continuidade operacional, além de dificultar a interoperabilidade entre os módulos e o gerenciamento centralizado das políticas de segurança

10.2. A solução UTM adotada contempla dispositivos físicos (appliances) de diferentes portes, todos gerenciados sob uma mesma suíte de segurança, além de licenças específicas e suporte técnico integrado. A eventual fragmentação da contratação entre múltiplos fornecedores implicaria riscos significativos à uniformidade técnica, à atualização sincronizada dos sistemas e à capacidade de resposta rápida a incidentes, dificultando também a responsabilização direta em casos de falhas operacionais ou de segurança.

10.3. A execução unificada da solução por um único fornecedor especializado assegura a consistência das configurações, a compatibilidade plena entre os equipamentos e a centralização do suporte técnico, fatores indispensáveis à manutenção de um ambiente seguro, confiável e eficiente. A contratação conjunta permite, ainda, maior eficiência na implantação, treinamento e monitoramento, reduzindo o tempo de estabilização da solução e garantindo a continuidade dos serviços prestados pela Defensoria Pública.

10.4. Diante disso, a adoção do regime de fornecimento por lote único se revela a única medida viável e tecnicamente adequada, alinhada aos princípios da economicidade, eficiência e segurança institucional. Tal estratégia assegura o atendimento integral aos requisitos de continuidade, disponibilidade e integridade das informações processadas e armazenadas no ambiente tecnológico 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 das soluções UTM atualmente em uso, bem como de tecnologias mais avançadas como NGFW. A devida iniciativa tem como objetivo fortalecer as competências técnicas dos servidores responsáveis pela segurança da informação, assegurando a correta operação, manutenção e evolução das ferramentas tecnológicas adotadas, em consonância com as exigências crescentes de proteção de dados e resiliência institucional.

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/6#ChegadaCorregedoria), 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 UTM (Unified Threat Management), a Defensoria Pública do Estado do Amapá pretende

fortalecer a proteção do seu ambiente de rede por meio de uma plataforma integrada e multifuncional. O principal resultado esperado é o aumento da resiliência contra ameaças cibernéticas internas e externas, assegurando a proteção dos dados institucionais sensíveis e proporcionando maior controle sobre o tráfego de rede, aplicações, usuários e conteúdos acessados.

13.2.A adoção da solução UTM também visa otimizar a gestão da segurança da informação por meio de uma administração centralizada, que inclui monitoramento contínuo, geração de relatórios automatizados, análise de logs e aplicação unificada de políticas. Isso resultará em maior eficiência operacional da equipe de tecnologia da informação, com capacidade aprimorada de prevenção, detecção e resposta a incidentes, além de contribuir para a redução de falhas, interrupções de serviço e vulnerabilidades técnicas.

13.3. Por fim, espera-se que a nova solução proporcione maior padronização e escalabilidade à infraestrutura de segurança da Defensoria, contemplando de forma uniforme todas as unidades — sede, anexos e núcleos regionais. A utilização de uma tecnologia unificada e compatível entre os diferentes appliances facilitará futuras expansões, atualizações e manutenção preventiva, garantindo a continuidade dos serviços públicos com qualidade, estabilidade e proteção, mesmo diante do crescimento institucional ou de mudanças tecnológicas futuras.

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 ARAUJO 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

[1] Um firewall é um sistema de segurança de rede projetado para monitorar, filtrar, permitir ou bloquear o tráfego de dados entre redes — especialmente entre uma rede interna confiável (como a de uma organização) e redes externas não confiáveis (como a internet). Seu principal objetivo é proteger os sistemas e dados contra acessos não autorizados, ataques cibernéticos, vazamento de informações e outras ameaças.

[2] Ransomware é um tipo de malware (software malicioso) que bloqueia ou criptografa os dados de um sistema, dispositivo ou rede, impedindo o acesso às informações até que a vítima pague um resgate (ransom) — geralmente exigido em criptomoedas como Bitcoin.

[3] A LGPD é a lei brasileira que estabelece regras sobre a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade do indivíduo. (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm)

[4] Segurança cibernética (ou cibersegurança) é o conjunto de práticas, tecnologias e processos utilizados para proteger sistemas, redes, dispositivos e dados digitais contra acessos não autorizados, ataques cibernéticos, danos ou roubos.

[5] O Firewall UTM da WatchGuard é uma solução integrada de segurança de rede que reúne múltiplas funcionalidades essenciais em um único appliance, proporcionando uma proteção abrangente e centralizada contra ameaças cibernéticas. A tecnologia UTM combina recursos como firewall tradicional, prevenção contra intrusões (IPS), antivírus, filtro de conteúdo web, controle de aplicações, VPN, detecção e bloqueio de malware, além de monitoramento e geração de relatórios em tempo real.

[6] Prevenção contra intrusões (IPS - Intrusion Prevention System) é uma tecnologia de segurança de rede projetada para identificar, analisar e bloquear automaticamente tentativas de ataques ou acessos não autorizados em tempo real. Diferente do IDS (Intrusion Detection System), que apenas detecta e alerta sobre ameaças, o IPS atua ativamente para impedir que essas ameaças comprometam sistemas e dados.

[7] No contexto de tecnologia da informação, modelos de appliance referem-se às variações específicas de equipamentos físicos (hardware) pré-configurados e otimizados para executar funções dedicadas, como segurança de rede, armazenamento, virtualização, entre outros.

[8] Throughput é a quantidade efetiva de dados que um sistema, rede ou dispositivo consegue processar, transmitir ou receber em um determinado período de tempo, geralmente medido em bits por segundo (bps), megabits por segundo (Mbps) ou gigabits por segundo (Gbps).

[9] Cloud Management, ou Gerenciamento na Nuvem, refere-se ao uso de plataformas e ferramentas baseadas na nuvem para administrar, monitorar, configurar e controlar sistemas, aplicações e dispositivos de forma remota e centralizada.

[10] Uma VPN (Rede Privada Virtual) é uma tecnologia que cria uma conexão segura e criptografada entre um dispositivo e uma rede, geralmente pela internet. Essa conexão permite que usuários ou filiais acessem recursos internos de uma rede privada de forma segura, mesmo estando em locais remotos ou públicos.

[11] O IPSec é um conjunto de protocolos que oferece segurança para o tráfego IP através de mecanismos de autenticação, integridade, confidencialidade (criptografia) e proteção contra replay. Ele é amplamente usado para criar VPNs site-to-site ou remote access VPNs que protegem a comunicação entre redes ou entre usuários remotos e a rede

[12] O SSL (atualmente sucedido pelo TLS) é um protocolo que provê segurança para comunicação em aplicações, especialmente em navegadores web e aplicativos, garantindo a criptografia dos dados transmitidos.

[13] Escalabilidade é um conceito utilizado em tecnologia da informação para descrever a capacidade de um sistema, rede ou solução crescer e se adaptar ao aumento da demanda sem perder desempenho ou eficiência

[14] Firmware é um tipo de software embutido diretamente no hardware de um dispositivo eletrônico, responsável por controlar, gerenciar e operar suas funções básicas. Ele funciona como uma ponte entre o hardware físico e o software de alto nível (como sistemas operacionais e aplicativos).

[15] Malware (abreviação de malicious software ou software malicioso) é qualquer tipo de software desenvolvido com a intenção de causar danos, comprometer sistemas, roubar informações ou controlar dispositivos sem autorização do usuário.

[16] O Sistema de Prevenção de Intrusão (IPS - Intrusion Prevention System) é uma tecnologia de segurança de rede que monitora o tráfego em tempo real, identifica atividades suspeitas ou maliciosas e atua automaticamente para bloquear ou impedir que essas ameaças comprometam sistemas e dados.

[17] Phishing é uma técnica de fraude digital utilizada por criminosos cibernéticos para enganar pessoas e obter informações sensíveis, como senhas, dados bancários, números de cartão de crédito e dados pessoais. Essa fraude normalmente ocorre por meio de mensagens falsas, que podem ser enviadas por e-mail, SMS, redes sociais ou outros canais de comunicação.

[18] DDoS, ou Ataque Distribuído de Negação de Serviço, é um tipo de ataque cibernético em que múltiplos computadores ou dispositivos — muitas vezes infectados por malware e controlados por hackers (botnets) — enviam um volume massivo de tráfego malicioso simultaneamente para um servidor, rede ou serviço online.

[19] http://comprasnet.gov.br/ConsultaLicitacoes/

[20] http://comprasnet.gov.br/ConsultaLicitacoes/

[21] Stateful Inspection, também conhecido como Inspeção com Estado, é uma técnica avançada usada em firewalls para monitorar o estado e o contexto das conexões de rede. Diferente dos firewalls tradicionais que analisam apenas os pacotes individualmente (stateless), o stateful inspection acompanha o estado da conexão — como início, andamento e término — permitindo decisões de filtragem mais inteligentes e seguras.

[22] Threat Intelligence é o conhecimento baseado em evidências — como indicadores de comprometimento, táticas de ataque, origem de ameaças e padrões de comportamento de agentes maliciosos — que ajuda organizações a tomar decisões informadas sobre segurança.

[23] SSL Inspection (ou inspeção SSL) é um processo de segurança em que o tráfego de dados criptografado por SSL/TLS (como o usado em sites com "https://") é interceptado, descriptografado, inspecionado e recriptografado antes de seguir para o destino final.

[24] Deep Packet Inspection (DPI), ou Inspeção Profunda de Pacotes, é uma técnica avançada de segurança de rede que analisa o conteúdo real dos pacotes de dados, indo além dos cabeçalhos padrão usados em inspeções tradicionais.

[25] Artigo 23, II - 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, observado o índice de atualização de preços correspondente; (Art. 23 da Lei nº 14.133/21); Artigo 5 º, II - 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, observado o índice de atualização de preços correspondente; (INSTRUÇÃO NORMATIVA SEGES/ME Nº 65, DE 7 DE JULHO DE 2021); Artº 3º , II - 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. PORTARIA Nº 35, DE 10 DE JANEIRO DE 2024.

[26] Artigo 23, III - utilização de dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que contenham a data e hora de acesso; (Art. 23 da Lei nº 14.133/21); Artigo 5 º, III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso; (INSTRUÇÃO NORMATIVA SEGES/ME Nº 65, DE 7 DE JULHO DE 2021); III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal ou estadual e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;

[27] Artigo 23, IV - pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; (Art. 23 da Lei nº 14.133/21); Artigo 5º, IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; (INSTRUÇÃO NORMATIVA SEGES/ME Nº 65, DE 7 DE JULHO DE 2021); Art 3º,IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital. PORTARIA Nº 35, DE 10 DE JANEIRO DE 2024.

Documento assinado eletronicamente por **rogerio leite moresco**, **COORDENADORIA DE LICITAÇÕES, CONTRATOS E CONVÊNIOS**, em 21/08/2025, às 09:20, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Walter Araujo Filho**, **COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO**, em 21/08/2025, às 09:44, 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 **0132750** e o código CRC **449BF4D4**.
