LABORATORIO NACIONAL DE ASTROFISICA - MG

Estudo Técnico Preliminar 47/2025

1. Informações Básicas

Número do processo: 01204.000236/2025-89

2. Descrição da necessidade

Este estudo trata da renovação da garantia, suporte e licença dos firewalls do Laboratório Nacional de Astrofísica (LNA) pelo período de 12 (doze) meses .

Com o avanço constante da tecnologia cibernética, maior utilização de sistemas computacionais e o crescente número de usuários conectados à Internet e, por consequência, sua exposição a ameaças, se mostra cada vez mais importante o investimento em segurança de redes de computadores. Este tipo de investimento é ainda mais importante levando em conta a existência de novas leis como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que apresenta as seguintes exigências:

> *Art. 46.* Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Hoje, todo o LNA é baseado em firewalls do tipo NGFW (*Next Generation Fiewall*) os quais permitem recursos adicionais quando comparado com o modelo tradicional. O modelo tradicional emprega bloqueio de portas e serviços como ação principal. Por outro lado, firewalls NGFW, adotado também em diversos órgãos federais, têm avanços tecnológicos tais como inspeção de pacotes, visibilidade de aplicações independente de protocolos e portas. Assim, é de fundamental importância manter os firewalls atualizados e com licenças de suporte ativas para proteger os dados na rede da Instituição.

Atualmente, esses NGFWs funcionam como segurança perimetral de borda e sem as licenças de suporte e atualizações a solução não permite o uso do filtro web, a atualização dos sistemas operacionais, serviços de filtragem e análise de pacotes o que reduz drasticamente a proteção da rede de dados da instituição. Para garantir a segurança dos dados transmitidos e armazenados na infraestrutura de rede, é fundamental renovar as licenças de firewall. Os modelos adotados de NGFW é do Fabricante Fortinet, sendo duas unidades do modelo FortiGate 80-F, para a sede do LNA e para o Observatório do pico dos Dias - OPD. A atualização das licenças garante a proteção dos dados e serviços como filtro de conteúdo web, e softwares de gerenciamento de logs e relatórios. Este estudo trata da renovação das licenças de firewall de toda o LNA que se encerrarão em outubro (FortiGate 80-F). Por outro lado, a aquisição está alinhada ao planejamento da organização, tal como mostram as tabelas 1 e 2.

Por meio deste estudo técnico, a instituição busca identificar a melhor forma de contratar uma empresa especializada no fornecimento de soluções de segurança de informação para proteger a rede LAN e WAN da instituição. O objetivo é garantir a confidencialidade, integridade e disponibilidade dos dados transmitidos ou armazenados na infraestrutura de rede da instituição, gerenciando riscos e ameaças aos ativos de tecnologia da informação. A interrupção dos serviços de tecnologia da informação pode afetar significativamente a operação da Instituição. Portanto, a renovação das licenças de firewall é crucial para garantir que o execução das atividades técnico-gerenciais, técnico-administrativas e de pesquisa científica continuem sem interrupções e para manter a segurança dos dados do LNA.

Tabela 1. Alinhamento ao PDTIC 2025

P-05	**Necessidade 03: Adquirir e/ou renovar licenças de softwares diversos para atender às demandas de todas as áreas da instituição.**			
Meta	Descrição	Indicadores	Valor	Prazo
M01	Manter atualizadas as licenças de softwares diversos para atender às demandas de todas as áreas da instituição.	% das licenças atualizadas	100%	Dez /2025

Tabela 2 Alinhamento ao PAC 2025

Item	**Descrição do item do PAC**
DFD 175/2024	Manutenção de software 2025

3. Área requisitante

Área Requisitante	Responsável
DIRETORIA	Ivanildo Faria Santiago

4. Necessidades de Negócio

Tabela 4. Identificação das necessidades de negócio.

ID	Descrição
1	Atender a demanda crescente por prevenção e mitigação de incidentes de segurança da informação
2	Garantir a adequação dos serviços de TI com os atos normativos do Governo Federal (LGPD, marco civil da internet, política nacional de segurança da informação, etc.)
3	Manter a disponibilidade, integridade e confiabilidade dos sistemas e aplicações da instituição
4	Garantir o funcionamento da rede institucional em regime de 24x7 ininterruptamente, com troca de equipamentos em até 24 horas após notificação do fabricante

5. Necessidades Tecnológicas

Tabela 5. Identificação das Necessidades Tecnológicas.

ID	Descrição
1	Monitorar e definir controles de segurança para o tráfego de dados da rede institucional
2	Garantir o gerenciamento por meio de interface Web e linha de comando (CLI)
3	Manter os logs da solução
4	Permitir acessos remotos através de IPsec VPN e SSL-VPN
5	Garantir soluções de VPN e site-to-site

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Tabela 6: Demais requisitos necessários e suficientes à escolha da solução de TIC.

ID	Descrição
1	A Solução deve ser capaz de registrar de forma centralizada todos os registros de conexões dos equipamentos ligados na rede institucional
2	A solução deve ser capaz de manter atualizada as assinaturas de vulnerabilidades e ameaças de forma automática
3	A solução deve permitir acessos gerenciados por meio de perfis de usuários distintos
4	A solução deve ser capaz de atender uma vazão de tráfego de rede

7. Estimativa da demanda - quantidade de bens e serviços

O LNA oferece uma infraestrutura de Tecnologia da Informação (TI) em 2 (duas) unidades com acesso a internet. A Oficina de Informática é responsável por planejar, executar e manter políticas e medidas que garantam a segurança e proteção da rede de dados e dos sistemas computacionais da instituição.

Até o ano 2022, a LNA utilizava uma solução de firewall baseada no fabricante CISCO, denominada ASA. Esse firewall oferecia um nível básico de proteção, diante da dimensão e grande fluxo de informações trafegadas na rede do LNA. A proteção da rede implementada no ASA era baseada na filtragem de pacotes, aplicando regras de bloqueios nas camadas de rede e transporte do modelo OSI. Dessa forma, ele atuava apenas com base nos cabeçalhos dos pacotes da camada de rede (IPv4, IPv6 e ICMP) e da camada de transporte (UDP e TCP). Assim, era possível criar regras apenas com base nos endereços IP (origem e/ou destino), portas (origem e/ou destino) e protocolos citados anteriormente.

Em 2022, foi realizado um processo de compra para a aquisição de uma solução de Firewall de Próxima Geração, ou, Next Generation Firewall (NGFW). A vencedora do certame forneceu equipamentos produzidos pelo fabricante Fortinet. Consequentemente, o LNA possui um conjunto de firewalls, com todos os equipamentos NGFW, operando de forma integrada, conectando e integrando todas as unidades da organização e operando entre as redes de dados internas, de cada unidade, e a internet, realizando a proteção contra ameaças externas e inspecionando o tráfego que tem como origem ou destino a internet.

A disponibilidade da rede de computadores é crucial para a maioria dos serviços e operações fundamentais do LNA. A segurança desses ambientes é um elemento crucial para garantir a continuidade desses serviços e evitar possíveis paralisações que poderiam ter um impacto negativo no desempenho institucional. Com o constante avanço da tecnologia, novas formas de ataques cibernéticos são descobertas diariamente, tornando essencial a revisão constante dos processos de segurança da informação e a incorporação de novas abordagens de segurança à infraestrutura de TI. Portanto, a rede e a internet desempenham um papel essencial, tornando a segurança da informação uma preocupação constante.

Além da importância da rede e da internet para o funcionamento do LNA, esses recursos também são fundamentais para muitos trabalhos atuais, principalmente durante e após a COVID-19. Com o aumento do trabalho remoto e da necessidade de comunicação e colaboração online, a rede e a internet se tornaram ainda mais essenciais para manter a produtividade e o desempenho de diversas organizações.

No caso do LNA, a rede e a internet são utilizadas para diversas finalidades, como o acesso a sistemas de governo e administrativos, comunicação entre os diferentes setores e unidades da organização, realização de videoconferências, armazenamento e compartilhamento de documentos, entre outras atividades. A dependência desses recursos é tão grande que qualquer interrupção na rede pode afetar diretamente o trabalho de dezenas de pessoas.

Diante disso, o LNA tem investido cada vez mais em medidas de segurança e proteção da sua rede e dos seus sistemas, por meio de políticas e práticas que visam minimizar o risco de ataques cibernéticos e garantir a integridade e confidencialidade dos dados da instituição. Além disso, o LNA busca sempre estar atualizada em relação às novas tecnologias e tendências em TI, de forma a oferecer um serviço cada vez mais eficiente e seguro para seus servidores e colaboradores e para a sociedade em geral.

O firewall deverá atender os seguintes requisitos:

- suportar controles e criação de políticas por zona de segurança, porta/protocolo e aplicações, categorias de aplicações, usuários, grupos de usuários, endereço IP e redes;
- possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- permitir a liberação e/ou bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- inspecionar o payload de pacote com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
- permitir o bloqueio de vulnerabilidades e de exploits conhecidos;
- incluir proteção contra ataques de negação de serviços (DoS);
- detectar e bloquear a origem de port scans, possibilitando a criação de com exceções para endereços IPs de ferramentas de monitoramento da organização;
- suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação;
- permitir a visualização de resultados das análises de malwares Zero Day nos diferentes sistemas operacionais suportados.

Além disso, o firewall deverá oferecer a proteção conhecida como URL filtering, que analisa cada URL acessada pelos usuários. Esse tipo de proteção é importante para ajudar o usuário a se proteger ao acessar sites desconhecidos. Ataques de phishing estão se tornando muito populares, então uma forma de proteção é garantir que a URL que está sendo acessada é segura. Esse tipo de ataque, muitas vezes, tenta roubar as credenciais de um determinado usuário, através de páginas falsas e semelhantes a página original. Em relação a essa proteção o firewall deverá atender aos seguintes requisitos: suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL, classificar o nível de risco de URLs em níveis, classificar sites em mais de uma categoria, categorização de URL deve analisar toda a URL e não somente até o nível de diretório e bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução.

No entanto, os equipamentos do LNA estão com licença, garantia, suporte por vencer. Isso deixará o LNA vulnerável a ataques externos e sem recursos importantes do firewall conforme descrito acima. Por isso, é de fundamental importância para a segurança da rede a continuidade do investimento. A tabela 7 mostra esses equipamentos.

Tabela 7. Equipamentos de segurança perimetral do LNA.

Item	Equipamento	Número de Série
1	FORTIGATE-80F	FGT80FTK22026755
2	FORTIGATE-80F	FGT80FTK22026172

8. Levantamento de soluções

Tabela 8. Lista de soluções.

ID	Descrição da Solução (ou cenário)
I	Aquisição de novos Firewalls
II	Renovação de licenciamento, garantia e suporte dos Firewalls já existentes no LNA
III	Contratação de solução de firewall na modalidade de serviço
IV	Implementação de firewall na nuvem privada

9. Análise comparativa de soluções

SOLUÇÃO I - Aquisição de novos Firewalls

Embora os Firewalls de Próxima Geração sejam uma plataforma de rede integrada altamente eficaz para proteger as organizações contra ameaças cibernéticas, sua adoção não é uma tarefa simples. A aquisição financeira de soluções NGFW pode ser bastante onerosa, e a implementação desses sistemas pode requerer alto custo de treinamento para que a equipe de TI possa gerenciá-los adequadamente.

Além disso, o tempo necessário para implementar novas soluções de segurança pode ser um desafio para muitas organizações. A adoção de um NGFW requer a avaliação cuidadosa das necessidades de segurança da organização, a seleção do fornecedor certo e a implementação do sistema em toda a rede. Todas essas etapas consomem tempo e recursos consideráveis.

No entanto, apesar desses desafios, a implementação de soluções NGFW é fundamental para garantir a segurança da informação em organizações de todos os tamanhos. As soluções dos fabricantes líderes do mercado, como Palo Alto Networks, Fortinet, Check Point, Barracuda, Cisco, Forcepoint e Juniper Networks, são altamente eficazes e podem oferecer a proteção necessária contra as ameaças cibernéticas mais avançadas.

Apesar o processo de adoção de soluções NGFW possa parecer difícil e demorado, os benefícios são inúmeros. A implementação de um NGFW permite que as organizações se protejam contra ameaças cibernéticas avançadas, protejam seus dados e informações e reduzam os riscos de perda de dados ou violações de segurança. Em resumo, os NGFWs são uma peça fundamental no quebra-cabeça da segurança da informação e, apesar do alto custo de treinamento, aquisição financeira e tempo, seu valor para a segurança das organizações é inegável.

SOLUÇÃO II - Renovação de licenciamento, garantia e suporte dos Firewalls já existentes no LNA.

A segurança da informação é um dos tópicos mais importantes na era digital em que vivemos. Com o aumento constante das ameaças cibernéticas, é fundamental que as empresas e organizações mantenham seus sistemas e hardwares atualizados e com suporte de segurança.

Esses firewalls são essenciais para garantir a segurança dos enlaces de dados. Eles ajudam a prevenir ameaças cibernéticas, como ataques de phishing, malware e outras formas de ataques cibernéticos que podem comprometer a segurança dos dados e informações da organização.

Cada firewall é cuidadosamente selecionado de acordo com a necessidade de cada unidade, variando de acordo com o enlace de dados e a quantidade de servidores e colaboradores de cada localidade.

É importante destacar que, para manter a efetividade dos equipamentos e softwares de segurança da informação, é necessário renovar as licenças de suporte e garantia dos equipamentos e softwares periodicamente. Isso garantirá que a instituição mantenha o investimento realizado em segurança da informação ativo e operante, reduzindo os riscos de ataques cibernéticos e protegendo as informações sensíveis da instituição. A adoção de NGFWs da Fortinet, aliada à renovação da licença de suporte e garantia, são ações que demonstram o compromisso do LNA em manter sua rede segura e protegida contra ameaças cibernéticas.

SOLUÇÃO III - Contratação de solução de firewall na modalidade de serviço.

A contratação de soluções de TI na modalidade de serviço, como é o caso da solução de firewall, apresenta vantagens e desvantagens. Uma das vantagens é que a empresa contratada se responsabiliza pelo fornecimento, instalação, configuração, garantia, suporte e monitoramento do equipamento, o que pode liberar a equipe de TI da instituição para se dedicar a outras atividades críticas do negócio. Além disso, em algumas modalidades, o firewall fica hospedado na nuvem, o que pode reduzir a necessidade de investimento em infraestrutura física.

Por outro lado, há desvantagens em relação ao modelo de serviço. Na modalidade em que o firewall fica hospedado na nuvem, o pagamento da mensalidade varia de acordo com a quantidade de tráfego que é inspecionado e processado pelo firewall na nuvem, o que pode tornar a previsão orçamentária mais difícil. Já na modalidade em que o equipamento físico é instalado na rede do cliente, a mensalidade é fixa, mas o custo total do serviço pode ser maior do que se o equipamento fosse adquirido de forma tradicional, uma vez que a empresa contratada inclui o custo do equipamento e os serviços de garantia, suporte e monitoramento no preço mensal.

Outro ponto de atenção é que, em ambas as modalidades, o não pagamento da mensalidade pode acarretar na suspensão da prestação do serviço e remoção do equipamento. Como o firewall é um equipamento fundamental na proteção da rede de dados, a suspensão do serviço pode deixar a instituição exposta a ataques cibernéticos e sem acesso à internet, trazendo enormes prejuízos. Por isso, é importante que a instituição faça uma análise cuidadosa dos custos e benefícios antes de considerar um modelo de serviço para a solução de firewall.

SOLUÇÃO IV - Implementação de firewall na nuvem privada.

A implementação de firewall em nuvem privada é uma solução relativamente nova, que ainda não é conhecida em instituições públicas com infraestrutura de TI semelhante ao LNA. Essa modalidade de implementação é semelhante à solução apresentada na Solução III, mas utiliza uma nuvem privada, na qual o firewall utiliza os recursos disponíveis nessa nuvem para funcionar, sem a necessidade de enviar dados para a nuvem de uma empresa ou fabricante do firewall. No entanto, essa solução apresenta algumas limitações.

Para implementar o firewall em nuvem privada, é necessário que a organização possua um ambiente de nuvem que suporte essa implementação e tenha licenças de firewall disponíveis. Além disso, essa solução não elimina a necessidade de adquirir equipamentos, pois o firewall ainda precisa de recursos para funcionar corretamente, o que pode limitar sua eficácia em alguns casos. Portanto, é importante considerar essas limitações ao decidir implementar um firewall em nuvem privada.

10. Registro de soluções consideradas inviáveis

A existência de diversas soluções de TIC de diferentes fabricantes acarreta em aumento nos custos operacionais, por exemplo, com estoque de sobressalentes e treinamentos, além de inviabilizar o investimento com softwares de gerenciamento, já que softwares de gerência são proprietários e não possibilitam o monitoramento de soluções de fabricantes diferentes, ou seja, seria necessário a aquisição de tantos softwares quanto às marcas dos equipamentos em uso, o que nos conduz a algumas limitações. Tal entendimento já foi manifestado no ACÓRDÃO 2789/2019 – PLENÁRIO do Tribunal de Contas da União (TCU), ao grafar:

> *"A falta de padronização das tecnologias afeta o acúmulo de conhecimento e a disseminação de boas práticas, o que poderia reduzir as necessidades de capacitação de pessoal e tornar a troca de experiências e movimentação de pessoal mais eficiente. Além disso, diminui a possibilidade de o Estado tirar proveito do efeito escala como grande comprador de tecnologia, aumentando a pressão sobre os custos. Por fim, dificulta a interoperabilidade entre os ambientes, tornando-se um incentivo perverso à criação de silos de informação, o que tanto emperra a integração de dados para a prestação de serviços públicos eficientes, sem contar com o esforço adicional que impõe às áreas de TI para lidar com tais complexidades."*

Outrossim, destacamos pontos relevantes no que tange à aspectos financeiros, técnicos e humanos, como expostos abaixo:

Financeira: Ao se trabalhar com um parque de firewalls de diversos fabricantes, serão necessários treinamento distintos para operação dos equipamentos, que apesar de similares, cada fabricante trabalha com comandos particulares às interfaces adotadas em seu sistema operacional.

Técnica: Considerando-se que não seja possível a transferência de configurações para equipamentos de marcas distintas, sem a necessidade de alteração nas sintaxes dos comandos, o que impossibilita a substituição imediata, ocasionando maiores períodos de indisponibilidade em casos de falha. A atual solução de segurança da informação, as regras de configuração, filtros de prevenção, assinatura de ameaças e o software de gerenciamento de logs centralizado existente não serão compatíveis com uma solução de outro fabricante, o que obrigaria o LNA a adquirir novos equipamentos, novo gerenciador de configurações e uma nova ferramenta para análise de logs. Além do custo de aquisição, ainda existe o custo de operação e manutenção de mais uma ferramenta na instituição. Dificulta ainda o estabelecimento de processos de gerência do equipamento, inviabilizando a especialização da equipe para operação dos equipamentos e suas funcionalidades, visto que serão necessários diversos treinamentos para fabricantes distintos, com equipamentos e funcionalidades distintas que nem sempre irão garantir sua interoperabilidade.

Humana: Atualmente a equipe responsável pela administração da solução de segurança da informação institucional, conta com apenas 2 (dois) servidores, acostumados com a solução implementada atualmente no LNA (Fortinet), de forma que, seria necessário o treinamento de toda equipe caso fosse adotada uma solução de diferente fabricante.

Dentre as soluções levantadas, foram identificadas três que são consideradas inviáveis, quais sejam:

SOLUÇÃO I - Aquisição de novos Firewalls.

Nessa proposta, os equipamentos já adquiridos e que estão em funcionamento seriam substituídos. Como esses equipamentos foram adquiridos em 2022, com suporte e garantia de 36 meses. A aquisição de uma nova solução de NGFW (Next Generation Firewall) incluiria a aquisição do hardware, além da necessidade de aquisição das licenças de software, suporte e garantia e dos softwares de gerenciamento centralizado e armazenamento de logs com geração de relatórios. Ou seja, além de adquirir o objeto desta contratação, seria necessário a aquisição de novos hardwares, softwares e treinamentos para que a equipe possa operar a nova solução de maneira correta, o que eleva o custo da solução e o tempo necessário para sua implantação.

SOLUÇÃO III - Contratação de solução de firewall na modalidade de serviço.

Por se tratar de uma solução com contratação na modalidade de serviço, a qual depende de pagamentos mensais para a continuidade na prestação de serviço, tal contratação depende da disponibilidade de verbas destinadas a custeio.

A inclusão de mais uma despesa mensal na já escassa verba de custeio traria ainda mais problemas para a administração do orçamento, tendo em vista que outras verbas essenciais, como despesas de água e luz, já fazem uso da verba de custeio.

SOLUÇÃO IV - Implementação de firewall na nuvem privada.

Devido ao fato dessa solução utilizar uma nuvem privada, essa solução não é viável, visto que o LNA ainda não possui um ambiente de nuvem em sua infraestrutura de TI. Dessa forma, não se tem nenhuma previsão sobre a possibilidade de utilizar esse ambiente para implementar um serviço tão crítico e essencial como o firewall, devido aos recursos e resultados de performance que ele requer. Sendo assim, essa solução é considerada inviável.

11. Análise comparativa de custos (TCO)

Para a construção das duas soluções, empregou como metodologia a INSTRUÇÃO NORMATIVA SEGES/ME Nº 65, DE 7 DE JULHO DE 2021, que dispõe de modelo para obtenção de preços, como se segue:

Art. 6º Serão utilizados, como métodos para obtenção do preço estimado, o menor dos valores obtidos na pesquisa de preços, desde que o cálculo incida sobre um conjunto de três ou mais preços, oriundos de um ou mais dos
parâmetros de que trata o art. 5º, desconsiderados os valores inexequíveis,inconsistentes e os excessivamente elevados.

A Tabela 9 mostra o menor preço do item da Solução II.

Tabela 9.

Item	Equipamento	Quantidade	Unidade	Valor Unitário	Valor Total
1	- Renovações da garantia, suporte e licença dos firewalls Fortigate 80F; - Seriais inclusos na renovação: FGT80FTK22026755 e FGT80FTK22026172; - Licença Fortinet - FC-10-0080F-950-02-12 - UTP (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare) - 1 ano.	2	UN	R$ 8.983,60	R$ 17.967,20

12. Descrição da solução de TIC a ser contratada

Por meio de pesquisa de mercado a renovação das licenças, suporte e garantia dos equipamentos já existentes no ambiente da LNA, tal qual cenário da Solução II, se mostrou mais viável financeiramente e tecnologicamente se comparado com a aquisição de novos equipamentos. Os custos de renovação se mostraram menores ao custo de aquisição de novos equipamentos, sem ocasionar nenhuma perda de desempenho nos serviços de TIC disponibilizados pela instituição.

Pode-se destacar também que eventuais problemas relacionados ao hardware ou software da solução de segurança atual estarão com o mesmo fabricante, que será corresponsável pelo troca do equipamento ou suporte por meio de técnicos especializados. Para o LNA, haverá um único ponto focal para abertura de chamados e um único contrato de suporte para gerenciar.

Além do exposto, como referência de mercado para as principais soluções de Network Firewall, é válido tomar como base as avaliações feitas pela consultoria Gartner. O quadrante mágico para soluções de firewall mais recente é o de dezembro de 2022, onde a solução utilizada pela LNA se destaca como um dos líderes do mercado em seu segmento, acompanhada por outras duas soluções: Check Point Software Technologies e Palo Alto Networks. O cenário completo por ser visto a seguir (figura 1):

Figura 1. Quadrante mágico do Gartner para soluções de Firewall.

Figure 1: Magic Quadrant for Network Firewalls

Source: Gartner (December 2022)

Por fim, após análises técnicas, conclui-se que a renovação das licenças, garantias e suporte dos equipamentos de segurança da informação atuais do LNA do mesmo fabricante (Solução II) é a única solução viável para alcançar os objetivos que esta instituição pretende com esta aquisição, não sendo justificável tecnicamente a aquisição de novos equipamentos de fabricantes diferentes.

12.1. As políticas, os modelos e os padrões de governo.

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X

A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X

13. Estimativa de custo total da contratação

Valor (R$): 17.967,20

Na tabela 10 são apresentados os valor finais da estimativa total da contratação.

Tabela 10.

Item	CATSER	Equipamento	Quantidade	Unidade	Valor Unitário	Valor Total
1	27502	- Renovações da garantia, suporte e licença dos firewalls Fortigate 80F; - Seriais inclusos na renovação: FGT80FTK22026755 e FGT80FTK22026172; - Licença Fortinet - FC-10-0080F-950-02-12 - UTP (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare) - 1 ano.	2	UN	R$ 8.983,60	R$ 17.967,20

14. Justificativa técnica da escolha da solução

Conforme demonstrado ao longo deste estudo, o LNA vem expandindo a preocupação e investimentos voltados a garantir a segurança da informação. Após a aquisição dos equipamentos NGFW, verificou-se avanço significativo na proteção da rede de comunicação de dados, dos dispositivos (estações de trabalho e servidores) e também nas informações que trafegam na rede. Com a renovação das licenças será possível avançar a proteção a níveis recomendados nas melhores práticas citadas na literatura e já adotadas em instituições que visam proteger suas redes, ativos e informações.

A solução de firewall que a instituição já possui, se mostrou eficiente e confiável desde a sua implementação, atendendo aos requisitos técnicos de performance, tendo em vista o alto volume de tráfego, considerando ainda todos os requisitos de proteção contra ameaças modernas e avançadas ativados simultaneamente para proteção do ambiente de rede, além de relatórios detalhados e logs intuitivos para análises específica. Ao expandir essa solução, através da renovação das licenças, será possível planejar e implementar avanços significativos em termos de proteção e performance, observando e seguindo as melhores e mais modernas práticas citadas na literatura e utilizadas em instituições de diversos portes que prezam por garantir a segurança das informações e do ambiente computacional.

Outro aspecto importante para escolha dessa solução é os benefícios que a padronização de equipamentos apresenta. Por meio dela, os processos relacionados a gerenciamento, monitoramento e implementação de novas funcionalidades são facilitados, devido ao conhecimento já existente sobre a metodologia e funcionalidades da solução.

Nesse sentido, o LNA possui uma equipe reduzida de analistas que atuam na proteção da rede, os quais já possuem cursos voltados à administração e gerenciamento da solução de firewall já utilizada.

15. Justificativa econômica da escolha da solução

Considerando que o LNA possui equipamentos de firewall adquiridos previamente, os quais necessitam apenas da renovação das licenças de suporte para atualização, substituir a solução atual por uma nova de um fabricante diferente incorreria em um aumento significativo de custo, uma vez que haveria duplicação de gastos com hardware, além das licenças do novo fabricante. A fim de estar em conformidade com as políticas de segurança da informação estabelecidas pela instituição e preservar a continuidade do negócio, é necessário manter esses equipamentos e renovar as licenças.

Além dos aspectos relacionados às licenças, é importante ressaltar que a equipe já possui conhecimento sobre a solução de firewall atual. Dessa forma, não seria necessário adquirir treinamentos adicionais para a equipe, o que aumentaria significativamente o tempo e o custo envolvidos na implementação de uma nova solução. Além disso, o agente público que atua na equipe de segurança da informação, já receberam treinamento sobre a solução atual de firewall.

Como resultado, essas pessoas possuem o conhecimento necessário para implementar serviços de rede no Next Generation Firewall (NGFW) atual. Se fosse selecionada uma nova solução de firewall, de um fabricante diferente, seria necessário que todos a equipe que gerencia a solução de NGFW recebesse treinamento adicional. Isso acarretaria um aumento nos custos associados à contratação, o que poderia ser evitado por meio da manutenção da solução atual e da renovação das licenças necessárias.

16. Benefícios a serem alcançados com a contratação

- Contribuir para garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Aprimorar a segurança de TIC do LNA frente a ameaças sofisticadas;
- Possibilitar o controle de acesso e complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;
- Possibilitar o acesso remoto de maneira estável aos colaboradores de forma segura;
- Prestar os serviços de TIC mantendo a segurança adequada às informações organizacionais, principalmente quanto à garantia de disponibilidade e integridade dos dados necessários ao pleno funcionamento dos processos administrativos;
- Assegurar a sustentabilidade e desempenho dos serviços da instituição, conforme sua nova topologia e tráfego de rede e;
- Aumento da capacidade de resposta a incidentes de segurança.

17. Providências a serem Adotadas

Não existem providências a serem realizadas.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

Conforme apresentado no item 12, a alternativa escolhida foi a manutenção dos equipamentos atualmente utilizados na LNA.
Portanto, optou-se pela renovação do licenciamento, pela contratação de serviço de suporte técnico especializado.
As razões que motivaram essa escolha estão pormenorizadas nos itens 8, 9, 14 e 15 deste Estudo Técnico Preliminar.
Uma relação dos benefícios que a solução escolhida proporcionará ao LNA estão descritas no item 16.
Adicionalmente, destacamos que essa contratação está alinhada aos instrumentos estratégicos institucionais e governamentais, conforme apresentado no item 2.
Por fim, os integrantes requisitante e técnico, declaram o presente estudo técnico preliminar viável, considerando as informações apuradas nas análises técnica-funcional e econômica, desde que sejam adotadas as premissas e conclusões descritas neste estudo técnico preliminar.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

IVANILDO FARIA SANTIAGO

Equipe de apoio

Assinou eletronicamente em 09/09/2025 às 14:57:23.