

Estudo Técnico Preliminar 83/2024

1. Informações Básicas

Número do processo: 48051.000207/2024-91

2. Objeto

O objeto dessa contratação é o registro de preços para eventual aquisição de “Solução de Firewall de Próxima Geração (NGFW)” para suprir a demanda da ANM”.

3. Descrição da necessidade

Sobre o objeto,

A solução a ser contratada consiste no registro de preços para eventual aquisição de uma “Solução de Firewall de Próxima Geração (NGFW)” destinada a atender as necessidades da ANM.

Essa solução abrange não apenas a aquisição de dois appliances de firewall, mas também os serviços essenciais para sua implementação e operação. Esses serviços incluem instalação, configuração, treinamento, além de um pacote de "Horas de Serviço Técnico" (HST) na modalidade de operação assistida e a utilização de um console de gerenciamento do firewall, oferecido como SaaS (Software como Serviço). Os serviços de instalação, configuração e treinamento serão realizados exclusivamente no primeiro ano, enquanto o console de gerenciamento e a operação assistida terão vigência inicial de um ano, com possibilidade de renovação em conformidade com a legislação aplicável.

No processo licitatório, a solução a ser **contratada deve ser estruturada como um único grupo**, uma vez que os bens e serviços que a compõem possuem características técnicas que exigem integração total, sendo indispensável que sejam providos pelo mesmo fabricante e fornecedor. Essa abordagem assegura a plena compatibilidade entre os componentes da solução, garantindo que os equipamentos de firewall de próxima geração (NGFW), os serviços de instalação, configuração, treinamento, operação assistida, e o console de gerenciamento funcionem de forma integrada, sem interrupções ou falhas decorrentes de incompatibilidades técnicas.

Além disso, a contratação unificada promove a eficiência na gestão do contrato, facilita o suporte técnico e a resolução de eventuais problemas, e assegura que todas as entregas estejam alinhadas com os padrões e requisitos estabelecidos pela Administração. A solução integrada é, portanto, essencial para garantir a funcionalidade, a segurança e o desempenho esperado, atendendo integralmente às necessidades da ANM.

A solução deverá ainda contemplar os seguintes requisitos:

- **Conformidade com Regulamentações:** A solução deve estar em conformidade com regulamentações relevantes da indústria e legislações de privacidade de dados, como GDPR, HIPAA, PCIDSS, entre outras, para garantir que a organização esteja em conformidade com requisitos legais e regulatórios.
- **Proteção de Dados Sensíveis:** O NGFW deve oferecer recursos avançados de proteção de dados sensíveis, garantindo a confidencialidade, integridade e disponibilidade das informações críticas da organização.
- **Segurança de Aplicações Críticas:** A solução deve ser capaz de proteger aplicações críticas de negócios contra ameaças cibernéticas, garantindo a disponibilidade e o desempenho dessas aplicações.
- **Resiliência e Continuidade de Negócios:** O NGFW deve ser resiliente a falhas e capaz de manter a continuidade das operações mesmo em caso de eventos adversos, como ataques DDoS ou falhas de hardware.
- **Escalabilidade e Crescimento:** A solução deve ser escalável para acompanhar o crescimento da organização, suportando um aumento no número de usuários, dispositivos e tráfego de rede sem comprometer o desempenho ou a segurança.
- **Gestão Eficiente e Simplificada:** O NGFW deve oferecer ferramentas de gestão eficientes e simplificadas, permitindo que os administradores configurem e monitorem a segurança da rede de forma centralizada e intuitiva.
- **Integração com Infraestrutura Existente:** É crucial que a solução seja facilmente integrada com a infraestrutura de TI existente da organização, incluindo sistemas de gestão de identidade, servidores de diretório, sistemas de monitoramento de segurança, entre outros.

- Custoefetividade: A solução deve oferecer um bom custobenefício, equilibrando os custos iniciais de aquisição e implementação com os benefícios de segurança e eficiência operacional a longo prazo.

Contexto da ANM,

A Agência Nacional de Mineração ANM, autarquia especial vinculada ao Ministério de Minas e Energia e criada pela Lei 13.575 /2017, desempenha um papel crucial na gestão dos recursos minerais do Brasil. Responsável por um setor econômico que contribui com 2 a 5% dos valores presentes na Balança Comercial brasileira, a ANM opera uma variedade de sistemas informatizados essenciais para suas operações diárias.

Entre esses sistemas, destacam-se o Sistema de Cadastro Mineiro, Sistema de Arrecadação e Sistema de Relatório Anual de Lavra, todos acessíveis via internet e amplamente utilizados pelo setor regulado. Além disso, muitos dos serviços da ANM são disponibilizados remotamente através do portal gov.br, exigindo uma infraestrutura de rede segura para proteger os dados sensíveis dos usuários.

Internamente, a ANM depende do acesso seguro a sistemas vitais, tais como o SEI Sistema Eletrônico de Informações, responsável pelo trâmite de processos minerários e administrativos, sistemas administrativos, servidores de email, servidores de aplicação, storages, virtualizadores e demais componentes de redes. A segurança dessas aplicações não apenas protege os dados empresariais dos regulados, mas também garante a confidencialidade, confiabilidade e integridade das informações internas da ANM.

O objetivo desta licitação é a aquisição de uma solução de firewall de próxima geração (Next Generation Firewall NGFW), que compreende a obtenção de novos appliances de firewall, um console de gerenciamento e monitoramento, bem como os serviços de instalação e configuração do firewall de próxima geração, juntamente com o treinamento oficial correspondente. Essa solução proporcionará à Agência um controle mais eficiente e seguro sobre o tráfego de rede, permitindo uma gestão mais adequada das comunicações e a proteção dos dados contra ameaças cibernéticas.

A substituição dos equipamentos em uso é vital devido a diversos fatores que afetam negativamente nosso ambiente de rede. Isso inclui a obsolescência dos dispositivos anteriores, sua incompatibilidade com tecnologias modernas, a falta de garantia e atualizações, os custos elevados de manutenção e suporte técnico, e o aumento do risco de segurança. Utilizar equipamentos desatualizados e sem suporte eleva consideravelmente o risco de segurança da nossa rede.

Essa atualização é fundamental para garantir a segurança, integridade e eficiência dos nossos sistemas e dados. Os dispositivos novos proporcionarão uma infraestrutura de rede mais confiável, compatível com as demandas atuais e futuras da Agência Nacional de Mineração (ANM). Essa medida é essencial para proteger tanto os dados da agência quanto dos regulados, assegurando a confidencialidade e disponibilidade das informações críticas para nossas operações.

A definição do número de appliances (4 unidades) reflete uma abordagem estratégica e cuidadosa na modernização da topologia de rede da Agência. Essa decisão foi baseada em uma análise detalhada das necessidades reais de tráfego, levando em consideração as características da infraestrutura física existente. A atual infraestrutura conta com equipamentos cujo throughput bruto foi estimado em 80 Gbps à época da aquisição (2015), mas a nova solução proposta não visa replicar esse valor específico. A definição dos requisitos de desempenho foi revista à luz das necessidades reais de tráfego da ANM, com base em métricas atualizadas de segurança, inspeção SSL, controle de aplicações, e sessões simultâneas, conforme estabelecido no Anexo A do Termo de Referência.

A atualização da topologia de rede, embasada em dados concretos, assegura que os novos equipamentos sejam dimensionados de forma adequada para garantir um desempenho superior, alta disponibilidade e escalabilidade. Isso resultará em uma infraestrutura de rede robusta e preparada para atender às necessidades da Agência de maneira eficaz e eficiente. Além disso, a atualização é esperada para ser mais econômica e vantajosa em comparação com a infraestrutura atualmente em uso. Essa proposta oferece uma excelente capacidade de redundância e resiliência, o que significa que, em caso de falha em um dos appliances, o tráfego pode ser facilmente redirecionado para evitar interrupções na conectividade.

O objeto dessa contratação solução de Firewall de Próxima Geração ou NextGeneration Firewall [NGFW] é uma evolução dos tradicionais firewalls, projetados para oferecer proteção avançada contra ameaças cibernéticas em redes corporativas. Eles combinam as funcionalidades de um firewall tradicional com recursos adicionais de segurança, como inspeção profunda de pacotes, prevenção contra intrusões (IPS), filtragem de conteúdo, controle de aplicativos e visibilidade avançada do tráfego de rede.

Com o crescente aumento da demanda por largura de banda nas redes corporativas, impulsionado pelo uso cada vez maior de aplicativos baseados na nuvem, videoconferências, streaming de mídia e outras atividades de alta largura de banda, os firewalls de próxima geração se tornaram essenciais. Eles são capazes de lidar com o tráfego intenso e complexo dessas aplicações, garantindo ao mesmo tempo a segurança da rede.

Além disso, os NGFWs são projetados para enfrentar as ameaças virtuais em constante evolução que as organizações enfrentam atualmente. Com recursos avançados de detecção e prevenção de ameaças, como análise comportamental, detecção de malware avançado e inteligência de ameaças em tempo real, esses firewalls são capazes de proteger as redes corporativas contra ataques sofisticados e em constante mutação.

Para os setores públicos, como órgãos governamentais e agências reguladoras, a segurança cibernética é uma prioridade máxima devido à natureza sensível dos dados e informações que manipulam. O uso de firewalls de próxima geração é crucial para garantir a proteção desses dados contra ameaças virtuais, ataques de hackers e violações de segurança. Eles proporcionam uma camada adicional de defesa que é essencial em um cenário de ameaças cibernéticas cada vez mais sofisticadas e frequentes.

O uso de equipamentos defasados tecnologicamente e sem suporte, especialmente no caso de firewalls, expõe as organizações a uma série de riscos significativos em termos de segurança cibernética e operações de rede. Aqui estão algumas das principais consequências e riscos associados:

- **Vulnerabilidades de Segurança Não Corrigidas:** Equipamentos desatualizados não recebem mais atualizações de segurança, o que significa que vulnerabilidades recém-descobertas não são corrigidas. Isso deixa a rede suscetível a ataques de hackers, malware e outras ameaças cibernéticas.
- **Falta de Suporte Técnico:** Sem suporte técnico do fabricante, não há recursos disponíveis para resolver problemas de desempenho, bugs ou falhas operacionais. Isso pode resultar em interrupções prolongadas nos serviços de rede e dificuldade em resolver problemas técnicos.
- **Incompatibilidade com Novas Tecnologias:** Equipamentos defasados podem não ser compatíveis com as últimas tecnologias e padrões de rede, limitando a capacidade da organização de implementar novas soluções e se adaptar às mudanças no ambiente de TI.
- **Baixo Desempenho e Confiabilidade:** Com o passar do tempo, equipamentos mais antigos tendem a apresentar baixo desempenho e confiabilidade reduzida devido ao desgaste físico e obsolescência tecnológica. Isso pode resultar em tempo de inatividade não planejado e impacto negativo na produtividade dos usuários.
- **Falhas de Conformidade:** Equipamentos sem suporte podem não atender mais aos requisitos de conformidade regulatória ou padrões de segurança da indústria. Isso pode levar a penalidades regulatórias, perda de confiança dos clientes e danos à reputação da organização.
- **Exposição a Ameaças Emergentes:** Com a rápida evolução do cenário de ameaças cibernéticas, os equipamentos obsoletos podem não oferecer proteção adequada contra ameaças emergentes, como ataques de ransomware, phishing avançado e violações de dados.

A variedade de marcas e modelos de Firewalls de Próxima Geração (NGFWs) traz consigo desafios significativos em termos de gerenciamento, padronização e manutenção. A falta de uniformidade pode complicar a implementação de políticas de segurança consistentes e a administração eficaz da rede.

Considerando as demandas por desempenho, escalabilidade e redundância, a opção por dois appliances em redundância se mostra uma escolha sensata para atender às exigências da infraestrutura de rede. Essa configuração oferece um equilíbrio entre capacidade, disponibilidade e eficiência, garantindo um ambiente de rede confiável e preparado para lidar com as necessidades atuais e futuras da Agência, ao mesmo tempo que representa uma solução custobenefício atrativa.

A decisão de investir em novos NGFWs é respaldada por uma análise minuciosa das demandas presentes e pela preocupação com a segurança e a manutenção da infraestrutura de rede. Os equipamentos existentes, da marca Fortinet, estão desprovidos de garantia e suporte, representando um risco significativo para a conectividade do ambiente da ANM e para a segurança e disponibilidade dos dados e serviços oferecidos pela Agência. A obsolescência desses equipamentos não apenas compromete a segurança, deixando-os vulneráveis a ameaças cibernéticas, mas também impacta negativamente a manutenção, uma vez que a falta de peças de reposição e atualizações de firmware dificulta a resolução de problemas e a otimização do desempenho.

A aquisição de novos firewalls, com garantia e suporte atualizados, não só fortalecerá a segurança da rede, mas também possibilitará uma gestão mais eficaz, reduzindo a exposição a riscos e garantindo a continuidade operacional. Além de abordar as lacunas de segurança e manutenção, essa atualização proporcionará um ambiente mais resiliente, capaz de enfrentar os desafios tecnológicos do futuro com confiança.

4. Área requisitante

Área Requisitante	Responsável
Superintendência de tecnologia da Informação	Fabio Fernando Borges

5. Necessidades de Negócio

Necessidades de Negócio da ANM para a Aquisição de um Firewall NGFW,

A Agência Nacional de Mineração (ANM) enfrenta um cenário crescente de desafios relacionados à segurança cibernética e à proteção dos dados de seus usuários. As necessidades de negócio que justificam a aquisição de um firewall de última geração (NGFW) estão diretamente relacionadas à sua missão de manter a segurança operacional e de proteger informações críticas, assegurando que os serviços e sistemas da agência continuem a funcionar de maneira eficaz e resiliente. Essas necessidades incluem:

- **Proteção Contra Ameaças Cibernéticas Crescentes:** Com o aumento global das ameaças cibernéticas, incluindo ransomware, ataques direcionados e vazamentos de dados, é fundamental que a ANM disponha de uma solução robusta para prevenir, detectar e responder a ataques em tempo real. O atual firewall, sem suporte e atualizações, não consegue proteger contra as vulnerabilidades mais recentes, expondo a agência a riscos críticos.
- **Garantia da Continuidade Operacional:** A ANM depende de atualizações tecnológicas para realizar suas funções regulatórias e administrativas. Um NGFW oferecerá resiliência contra ataques como DDoS e permitirá a rápida mitigação de falhas de segurança, garantindo que os serviços essenciais continuem operacionais mesmo em cenários adversos.
- **Proteção de Dados e Conformidade Regulatória:** A agência lida com dados sensíveis, tanto de servidores internos quanto de sistemas usados por terceiros, que exigem alta confidencialidade e integridade. A aquisição de um NGFW permitirá o cumprimento de regulamentações como a Lei Geral de Proteção de Dados (LGPD) e padrões internacionais de segurança, assegurando conformidade e evitando sanções legais.
- **Segurança para Usuários Internos e Externos:** O crescimento no número de usuários conectados, seja de servidores, estações de trabalho ou dispositivos móveis, aumenta a superfície de ataque. O NGFW oferecerá controle granular de acessos, segmentação de rede e proteção contra ameaças voltadas a esses usuários, elevando o nível de segurança.
- **Capacidade de Crescimento e Integração:** Com uma infraestrutura tecnológica em expansão, a solução deve ser escalável para atender às demandas futuras da ANM. O NGFW escolhido deverá integrar-se perfeitamente com os sistemas existentes, oferecendo flexibilidade para acompanhar a evolução tecnológica e o crescimento da agência.
- **Gestão Centralizada e Eficiência Operacional:** A administração simplificada de políticas de segurança e a capacidade de monitorar a rede de maneira centralizada permitirão uma gestão mais eficiente. A integração de ferramentas avançadas, como detecção e resposta automatizadas, ajudará a equipe técnica da ANM a concentrar esforços em atividades estratégicas.

6. Necessidades Tecnológicas

A aquisição de um NGFW (Next-Generation Firewall) pela ANM deve atender a requisitos tecnológicos avançados, garantindo que a solução escolhida seja capaz de lidar com as demandas crescentes de segurança cibernética e proteção de dados. Os principais requisitos tecnológicos discutidos incluem:

Controle e Gerenciamento Granular

- **Segmentação de Rede:** Divisão da rede em zonas para limitar o alcance de ataques internos e melhorar a gestão de tráfego.
- **Controle de Aplicativos:** Identificação e controle do uso de aplicativos, garantindo que apenas softwares autorizados sejam executados na rede.

Atualizações e Suporte Contínuos

- **Atualizações Automáticas de Assinaturas de Ameaças:** O NGFW deve receber atualizações frequentes para proteger contra novas vulnerabilidades.
- **Suporte Técnico Prolongado:** Garantia mínima de 60 meses.

Escalabilidade e Desempenho

- **Capacidade de Crescimento:** O NGFW deve suportar aumentos de tráfego, usuários e dispositivos sem comprometer a segurança ou o desempenho.

- Alta Disponibilidade (HA): Configurações redundantes para garantir continuidade em caso de falhas.

Conformidade Regulatória e Proteção de Dados

- Adesão a Normas Locais e Internacionais: Conformidade com regulamentos como LGPD (Lei Geral de Proteção de Dados), GDPR, PCI-DSS, entre outros.
- Criptografia Avançada: Suporte a padrões como AES-256 para garantir a proteção dos dados em trânsito e em repouso.

Integração e Automação

- Compatibilidade com Infraestrutura Existente: Integração com sistemas de gestão de identidade, servidores de diretório e outras soluções de segurança.
- Automação e Resposta Rápida: Ferramentas para automação de tarefas e resposta a incidentes, otimizando os esforços das equipes de segurança.

Relatórios e Análise

- Monitoramento e Logs Centralizados: Interface única para visualizar atividades e gerar relatórios detalhados de ameaças e eventos.
- Inteligência de Ameaças: Uso de fontes de inteligência para melhorar a detecção e resposta às ameaças emergentes.

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

Requisitos de Negócio:

A presente contratação orienta-se pelos seguintes requisitos de negócio:

- Segurança da Informação e Continuidade Operacional: A solução contratada deverá garantir a proteção efetiva do ambiente tecnológico da ANM contra ameaças cibernéticas, por meio de mecanismos avançados de inspeção, prevenção e resposta a incidentes. O firewall deve assegurar alta disponibilidade, desempenho adequado e resiliência, de modo a não comprometer os serviços essenciais da Agência.
- Conformidade com Normas e Boas Práticas: A solução deverá atender aos princípios e diretrizes da segurança da informação preconizados pela Instrução Normativa SGD/ME nº 1/2020, pela Estratégia de Governo Digital (EGD) e pela Política Nacional de Segurança da Informação (PNSI), além de seguir boas práticas do mercado como NIST, ISO/IEC 27001 e ITIL no que couber.
- Governança e Visibilidade Operacional: É necessário que a solução contemple um console de gerenciamento centralizado, que permita à ANM acompanhar e auditar os eventos, políticas de segurança, atualizações e a performance dos dispositivos de forma contínua e estruturada.
- Capacitação e Transferência de Conhecimento: A operação assistida deverá prover o apoio necessário à equipe técnica da ANM para domínio da solução implantada, promovendo capacitação prática, documentação e suporte próximo, de forma a permitir a autonomia técnica da Agência ao final do processo.
- Evolução Tecnológica e Suporte Prolongado: A solução deve prever ciclo de vida mínimo de 60 meses com suporte técnico contínuo, acesso a atualizações de firmware e assinaturas de segurança, garantindo aderência às tecnologias emergentes e mitigação de riscos de obsolescência.
- Escalabilidade e Integração com Infraestrutura Existente: A arquitetura da solução deve possibilitar expansões futuras (como aumento de throughput, adição de módulos ou integração com sistemas legados) com o menor impacto possível, considerando as características do datacenter da ANM.
- Eficiência Orçamentária e Sustentabilidade Administrativa: A contratação deve assegurar o melhor custo-benefício em médio e longo prazo, alinhando previsibilidade orçamentária com racionalidade técnica e administrativa, sem comprometer a continuidade dos serviços prestados pela Agência.
- Conformidade com Regulamentações: A solução deve estar em conformidade com regulamentações relevantes da indústria e legislações de privacidade de dados, como GDPR, HIPAA, PCIDSS, entre outras, para garantir que a organização esteja em conformidade com requisitos legais e regulatórios.
- Proteção de Dados Sensíveis: O NGFW deve oferecer recursos avançados de proteção de dados sensíveis, garantindo a confidencialidade, integridade e disponibilidade das informações críticas da organização.
- Segurança de Aplicações Críticas: A solução deve ser capaz de proteger aplicações críticas de negócios contra ameaças cibernéticas, garantindo a disponibilidade e o desempenho dessas aplicações.
- Resiliência e Continuidade de Negócios: O NGFW deve ser resiliente a falhas e capaz de manter a continuidade das operações mesmo em caso de eventos adversos, como ataques DDoS ou falhas de hardware.

- Escalabilidade e Crescimento: A solução deve ser escalável para acompanhar o crescimento da organização, suportando um aumento no número de usuários, dispositivos e tráfego de rede sem comprometer o desempenho ou a segurança.
- Gestão Eficiente e Simplificada: O NGFW deve oferecer ferramentas de gestão eficientes e simplificadas, permitindo que os administradores configurem e monitorem a segurança da rede de forma centralizada e intuitiva.
- Integração com Infraestrutura Existente: É crucial que a solução seja facilmente integrada com a infraestrutura de TI existente da organização, incluindo sistemas de gestão de identidade, servidores de diretório, sistemas de monitoramento de segurança, entre outros.
- Custoefetividade: A solução deve oferecer um bom custobenefício, equilibrando os custos iniciais de aquisição e implementação com os benefícios de segurança e eficiência operacional a longo prazo.

Requisitos de Capacitação:

Para garantir a transferência efetiva de conhecimento e a plena operação da solução de firewall de próxima geração (NGFW), a CONTRATADA deverá fornecer treinamento, observando que:

- A CONTRATADA deverá indicar um técnico habilitado, com profundo conhecimento na solução NGFW ofertada, para ministrar o treinamento técnico especializado.
- A capacitação será destinada a uma turma de, no máximo, 10 (dez) técnicos indicados pela CONTRATANTE, abordando, de forma teórica e prática, os procedimentos essenciais de configuração, monitoramento, manutenção e resolução de incidentes, incluindo dentre outras, a migração de regras e a gestão das funcionalidades avançadas da solução.
- O treinamento deverá ter carga horária de até 48 (quarenta e oito) horas, realizado na modalidade remota (online), com metodologia e conteúdo programático definidos em conjunto com a CONTRATANTE, garantindo a padronização dos processos operacionais e a continuidade da infraestrutura de segurança.

Requisitos Legais:

O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

Requisitos de Manutenção:

- A CONTRATANTE notificará a CONTRATADA através de comunicação oficial na ocorrência de defeitos nos equipamentos fornecidos, durante o período de garantia estendida.
- A CONTRATADA deverá em até 5 (cinco) dias úteis a partir da notificação de que trata o parágrafo anterior, avaliar o equipamento que apresentou defeito e emitir Laudo Técnico de forma a reconhecer o defeito do equipamento ou comprovar a decorrência de mau uso.
- Reconhecido o defeito do equipamento, a substituição/reparo ocorrerá dentro de até 20 (vinte) dias úteis contados a partir da assinatura da comunicação oficial de que trata este item.
- Alegado defeito por mau uso, ficam os prazos da comunicação oficial suspensos até avaliação da CONTRATANTE do Laudo Técnico emitido pela CONTRATADA.
- A CONTRATANTE, mediante justificativa técnica, poderá acatar o Laudo Técnico da CONTRATADA ou rejeitá-lo, não cabendo recurso ao entendimento técnico emitido pela Superintendência de Tecnologia da Informação da CONTRATANTE.
- No caso da CONTRATANTE, de forma justificada, acatar o Laudo Técnico, fica a CONTRATADA desobrigada da substituição do equipamento, sendo a recuperação do ativo de responsabilidade da CONTRATANTE.
- No caso da CONTRATANTE, de forma justificada, rejeitar as alegações do Laudo Técnico, fica a CONTRATADA responsável pelo fornecimento de novo equipamento, em características idênticas ao equipamento defeituoso, nos períodos neste item previstos, retomada a contagem de prazo a partir da notificação oficial da CONTRATADA pela CONTRATANTE quanto à rejeição das alegações técnicas.

Justificativa: No contexto deste objeto, não temos o tipo de manutenção previsto no texto original da AGU. No entanto, aplica-se o tipo de manutenção demandada quando fizer uso da garantia. Por isso, foi necessário ajustar o texto para refletir essa especificidade, garantindo que a manutenção seja realizada conforme as condições da garantia, assegurando a continuidade e qualidade dos serviços e bens contratados.

Requisitos Temporais:

A Entrega dos equipamentos (item 1) deverá ser efetivada no prazo máximo de 15 dias corridos, a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante:

- Para a entrega dos appliances previstos no Item 1, a contratada deverá realizar a entrega inicial no datacenter da ANM, localizado nas dependências do SERPRO, em Brasília/DF. Após essa entrega, deverão ser executadas as atividades previstas no Item 3, referentes à instalação e configuração dos equipamentos. Concluída essa etapa, a equipe designada pela CONTRATANTE realizará os testes de conformidade. Sendo os resultados satisfatórios, será emitido o termo de recebimento provisório dos bens, seguido do processo de patrimonialização. Posteriormente, ocorrerá a emissão do termo de recebimento definitivo, o respectivo ateste e o pagamento. É de inteira responsabilidade da contratada garantir o transporte seguro (“moving”) dos equipamentos até o local indicado, devendo adotar todas as providências necessárias para assegurar que o deslocamento ocorra de forma segura e sem intercorrências.

Os serviços devem ser prestados, para os itens 2 e 3, no prazo máximo de 72 (setenta e duas) horas-a contar do recebimento da abertura da Ordem de Serviço (OS), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante; para o item 4, no prazo máximo de 5 (cinco) dias, a contar do recebimento da abertura da Ordem de Serviço (OS), emitida pela Contratante, para o item 5, no prazo definido no chamado de abertura do atendimento, feito pela Contratante, considerando o grau de severidade do problema.

Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

Requisitos de Segurança e Privacidade

A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante (definidas nas Resoluções ANM nº 53 e 54 de 2021 ou nas que vierem a substituí-las), observando sobretudo os requisitos abaixo:

- Controle de Acesso: Implementação de contas de acesso únicas, pessoais e intransferíveis, com senhas seguras e temporárias, e bloqueio de contas após tentativas malsucedidas ou períodos de inatividade. Garantir que apenas usuários autorizados tenham acesso aos sistemas e dados da ANM.
- Monitoramento e Auditoria: Manutenção de registros de auditoria (logs) para monitorar atividades da rede, incluindo acessos remotos e utilização de VPN. Esses registros devem permitir o rastreamento das ações tomadas para posterior auditoria, garantindo a integridade e segurança das informações.
- Acesso Remoto Seguro: Utilização de VPN para acesso remoto, com análise de riscos e autorização prévia. As conexões remotas devem ser seguras e monitoradas para evitar vulnerabilidades e garantir a proteção dos dados.
- Garantia de Segurança, Integridade e Disponibilidade das Informações: Implementação de medidas de segurança para proteger contra ameaças cibernéticas, garantindo a integridade e disponibilidade das informações manipuladas pela solução. Isso inclui a utilização de soluções de detecção e bloqueio de programas maliciosos, como antispysware e antivírus.
- Proteção à Privacidade dos Dados: Ampla proteção à privacidade dos dados da ANM, conforme a Lei Geral de Proteção de Dados Pessoais (LGPD). Isso inclui o mapeamento de dados pessoais, a finalidade do tratamento desses dados, e a forma de atendimento aos direitos do titular, como acesso, retificação, exclusão e revogação de consentimento.
- Sigilo nas Informações Acessadas: Garantir o sigilo das informações acessadas, assegurando que dados sensíveis sejam protegidos contra acessos não autorizados e vazamentos. A contratada deve seguir rigorosamente as normas de segurança da informação estabelecidas pela ANM.

Requisitos Sociais, Ambientais e Culturais:

Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

- Nos termos da Instrução Normativa nº 01, de 19 de janeiro de 2010, da SLTI, quando aplicável, a contratada deverá observar as seguintes práticas de sustentabilidade: (i) que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico e/ou biodegradável, conforme as normas ABNT NBR 15448-1 e 15448-2; (ii) que os bens estejam preferencialmente acondicionados em embalagem individual adequada, com o menor volume possível, utilizando materiais recicláveis, de forma a garantir proteção durante o transporte e armazenamento; (iii) que os bens não contenham substâncias perigosas em concentrações superiores às recomendadas pela diretiva RoHS, como mercúrio, chumbo, cromo hexavalente, cádmio, PBBs e PBDEs; e, (iv) para serviços contratados, que as empresas adotem, sempre que cabível, práticas que respeitem as normas brasileiras da ABNT relacionadas à gestão de resíduos sólidos.
- Durante a execução de tarefas no ambiente do CONTRATANTE ou das demais instituições públicas envolvidas, os colaboradores da empresa fornecedora deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público. Deverão ainda portar identificação pessoal, de acordo com as normas internas das instituições.

- Os produtos gerados em função da prestação dos serviços, bem como todas as documentações, deverão ser entregues no idioma português do Brasil (ptBR), com exceção de termos técnicos usuais que poderão ser apresentados em língua estrangeira.
- E ainda com o objetivo de promover uma relação contratual responsável e alinhada com os princípios de sustentabilidade, respeito aos direitos humanos, valorização da cultura e ética empresarial deverá observar na execução do objeto (sempre que couber) os seguintes requisitos:
- Responsabilidade Social: a) Observar e respeitar os direitos humanos, garantindo igualdade de oportunidades e não discriminação em todas as suas atividades. b) Promover a diversidade e a inclusão, valorizando a equidade de gênero, etnia, idade, orientação sexual e demais características individuais. c) Estimular a contratação de mão de obra local e a capacitação de profissionais da região, contribuindo para o desenvolvimento econômico e social.
- Sustentabilidade Ambiental: a) Adotar práticas sustentáveis em suas operações, promovendo a economia de recursos naturais, a redução da emissão de gases de efeito estufa e o uso eficiente de energia. b) Gerenciar de forma adequada os resíduos gerados durante a prestação dos serviços, priorizando a coleta seletiva, a reciclagem e a destinação correta. c) Respeitar e adotar normas ambientais vigentes, visando à preservação dos ecossistemas e à mitigação de impactos ambientais adversos.
- Preservação Cultural: a) Respeitar e valorizar a diversidade cultural local, observando as tradições, costumes e patrimônio histórico. b) Promover ações que valorizem a cultura regional.
- Transparência e Ética: a) Cumprir rigorosamente as leis, regulamentos e normas éticas relacionadas à prestação dos serviços, garantindo a integridade e a transparência em todas as atividades. b) Assegurar a confidencialidade das informações da Agência e dos dados dos usuários, implementando medidas adequadas de segurança da informação.

Requisitos da Arquitetura Tecnológica:

Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.

A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

Requisitos de Projeto e de Implementação:

Os serviços deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir :

- Análise de Requisitos: O fornecedor deve conduzir uma análise detalhada dos requisitos de segurança e de rede da organização para garantir que a solução NGFW seja dimensionada e configurada adequadamente para atender às necessidades específicas da organização.
- Projeto Personalizado: Deve ser desenvolvido um projeto personalizado que leve em consideração a topologia de rede existente, os requisitos de segurança, as políticas e procedimentos da organização, e quaisquer considerações regulatórias ou de conformidade.
- Testes de Aceitação: Antes da implementação, devem ser conduzidos testes de aceitação para garantir que a solução NGFW atenda aos requisitos e expectativas da organização em termos de desempenho, segurança e funcionalidade.
- Implantação Planejada: A implantação da solução NGFW deve ser cuidadosamente planejada e coordenada para minimizar interrupções no ambiente de rede e garantir uma transição suave para a nova infraestrutura.
- Configuração e Customização: O fornecedor deve configurar e personalizar a solução NGFW de acordo com os requisitos específicos da organização, incluindo políticas de segurança, regras de firewall, e integração com outros sistemas de segurança.
- Integração com Sistemas Existentes: A solução NGFW deve ser integrada de forma transparente com os sistemas de rede e segurança existentes da organização, garantindo interoperabilidade e compatibilidade com outros dispositivos e aplicativos.
- Treinamento e Capacitação: O fornecedor deve fornecer treinamento e capacitação para a equipe de TI da organização, garantindo que eles tenham o conhecimento e as habilidades necessárias para operar e manter a solução NGFW de forma eficaz.
- Documentação Detalhada: Deve ser fornecida documentação detalhada, incluindo manuais de usuário, guias de configuração e procedimentos operacionais padrão (SOPs), para facilitar a operação e manutenção da solução NGFW pela equipe de TI da organização.

Requisitos de Implantação:

Os equipamentos deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

- Para todos os produtos (hardware e software) disponibilizados pela Contratada, deverão ser fornecidos a instalação, a customização, a montagem física dos equipamentos e seus respectivos acessórios, bem como toda a configuração lógica.

- A instalação e configuração deverão ser realizadas por técnico certificado com capacidade técnica para a realização do serviço comprovada através da apresentação de documento de certificação emitido pelo próprio fabricante do equipamento ou por empresa de treinamento reconhecida pelo fabricante. A documentação de certificação do técnico deverá ser apresentada no máximo 05 (cinco) dias após a assinatura do contrato.
- A instalação deverá ocorrer na Sede da CONTRATANTE.
- Os equipamentos ofertados deverão ser instalados e configurados na estrutura do datacenter e LAN (Local Area Network) da CONTRATANTE, conforme parâmetros a serem definidos em conjunto com a Contratada.
- A instalação e configuração deverá seguir as melhores práticas para os equipamentos entregues pela Contratada e sua interoperabilidade com a infraestrutura da CONTRATANTE, evitando qualquer tipo de incompatibilidade.
- Deverá ser realizada em, no máximo, 05 (cinco) dias após a assinatura do contrato, reunião de kickoff para alinhamento das expectativas do projeto, com apresentação de cronograma com as estimativas de tempo para a realização das atividades.
- Nesta reunião deverão ser levantadas todas as informações necessárias a respeito do escopo dos serviços que serão executados, incluindo-se as necessidades de migração, viabilidade técnica e funcional, limitações e impactos, e submetê-las ao parecer da CONTRATANTE.
- As atividades definidas no projeto deverão ser executadas em prazo a ser definido entre CONTRATADA e CONTRATANTE, sendo que 50% do total de horas disponíveis poderão ser utilizadas para tarefas que geram indisponibilidade e que deverão ser realizadas em dias não úteis (sábado, domingo e feriados).

Deverão ser realizadas as seguintes atividades mínimas:

- Instalação física no Datacenter da CONTRATANTE.
- Configuração Inicial do sistema, incluindo configuração de acesso de gerenciamento ao sistema (usuários e senhas), configuração inicial dos equipamentos.
- Configuração de rede/VLAN.
- Realização de testes de funcionamento dos equipamentos.
- Realização de testes de funcionamento de acesso.
- Atualização do firmware/sistema operacional dos sistemas e equipamentos.
- Demais atividades necessárias para o perfeito funcionamento dos sistemas.
- A Contratada deverá em até 15 (quinze) dias após a instalação dos itens entregar documentação "AS BUILT", contendo todas as informações relativas a instalação, configuração, nova topologia, localização física no datacenter da CONTRATANTE, conexões físicas utilizadas, endereços IPs e nomenclaturas utilizadas, nomes de usuário e senhas, entre outras. Esta documentação deverá quando possível conter fotos.

Requisitos de Garantia e Manutenção:

Para o item 1, o prazo de garantia contratual dos bens, complementar à garantia legal, será de, no mínimo, 57 (cinquenta e sete) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

Relativo aos serviços, o prazo de garantia contratual, complementar à garantia legal, será de 9 (nove) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

Requisitos de Experiência Profissional

Os serviços definidos no objeto deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

Requisitos de Formação da Equipe

Os serviços deverão ser prestados por técnicos devidamente capacitados.

Requisitos de Metodologia de Trabalho

A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante, ou no caso do item 5, da abertura do "Chamado" de atendimento.

A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados, e o Chamado deverá indicar o grau de severidade do problema.

A execução do serviço deve ser acompanhada pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

Requisitos de Segurança da Informação e Privacidade

O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

- Normas de Segurança da Informação e Privacidade descritas na POSIC da ANM;
- Lei Nº 13.708, de 14 de agosto de 2018 Lei Geral de Proteção de Dados Pessoais;
- Decreto Nº 9.637, de 26 de dezembro de 2018 Institui a Política Nacional de Segurança da Informação;
- Instrução Normativa GSI/PR Nº 1, de 13 de junho de 2008 e suas normas complementares Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;
- Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020 e suas normas complementares Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
- Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021 e suas normas complementares Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal
- Norma Complementar Nº 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012 Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;
- Norma Complementar Nº 13/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, Diretrizes para gestão de mudanças nos aspectos relativos à segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal;
- Norma Complementar Nº 07/IN01/DSIC/GSIPR, de 15 de julho de 2014 Diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações;
- ABNT NBR ISO 22301:2013 Sistemas de gestão de continuidade de negócios;
- ABNT NBR ISO 22313:2015 Sistemas de gestão de continuidade de negócios;
- ABNT NBR ISO 27031:2015 Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação;
- ABNT NBR 11515:2007 Guia de práticas para segurança física relativas ao armazenamento de dados;
- ABNT NBR ISO/IEC 27002:2013 Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27014:2013 Governança de segurança da informação;
- A CONTRATADA não pode obter, capturar, copiar ou transferir qualquer tipo informação de propriedade da CONTRATANTE, sem autorização.
- A CONTRATADA deverá atender as Políticas de Segurança da Informação e demais normativos correlatos publicados pela CONTRATANTE, bem como assinar Termo de Compromisso e seus funcionários alocados na prestação de serviços, o Termo de Ciência e Termo de compromisso e manutenção de sigilo em contrato, conforme modelos anexos ao Termo de Referência.
- A propriedade intelectual e os direitos autorais dos dados e informações e qualquer tipo de trabalho relacionado às demandas da CONTRATANTE, serão de sua titularidade. A CONTRATADA deve abster de divulgar ou repassar quaisquer dados ou informações, salvo se expressamente autorizado pela CONTRATANTE.
- Outras medidas indicadas durante a vigência do contrato pela CONTRATANTE.

Vistoria

Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

Outros Requisitos Aplicáveis

Não se aplica.

Sustentabilidade:

Entende-se que não são aplicáveis, neste caso, os requisitos ambientais previstos no Guia Nacional de Contratações Sustentáveis (2024), considerando - baseado nas diretrizes desse normativo - que a avaliação de conformidade de bens de informática definida pela Portaria Inmetro nº 304, de 06 de novembro de 2023, que é de caráter voluntário (Art. 1º, §1º), não se justifica sua exigência nesta contratação, sob pena de comprometer a competitividade do certame, restringindo a participação de fornecedores cujos equipamentos, embora tecnicamente compatíveis, não tenham voluntariamente efetuado essa certificação, além disso, em relação aos serviços contratados, estes serão prestados exclusivamente de forma remota, não havendo impactos ambientais diretos que justifiquem exigências adicionais.

Justificativa: Já apresentada no texto acima.

Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021):

Não se aplica.

Da vedação de utilização de marca/produto na execução do serviço:

Não se aplica.

Da exigência de carta de solidariedade:

Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato. Esse documento deverá garantir que, mesmo na ausência de capacidade técnica ou operacional do revendedor ou distribuidor, o fabricante comprometa-se a dar suporte à execução contratual, resguardando a continuidade do fornecimento e a qualidade dos serviços ou bens contratados.

Justificativa Técnica para Exigência de Carta de Solidariedade,

A presente exigência de carta de solidariedade do fabricante no processo licitatório para aquisição de solução de firewall e serviços correlatos, em estrita observância aos princípios da eficiência, segurança e continuidade dos serviços públicos se justifica sobretudo por:

- **Complexidade Tecnológica e Especificidade da Solução:** A solução de firewall representa um componente crítico da infraestrutura de tecnologia da informação e segurança cibernética, dada a complexidade dos sistemas de proteção de redes e a necessidade de garantir compatibilidade, integração e desempenho otimizado, torna-se imperativo assegurar suporte direto e integral do fabricante.
- **Continuidade e Tempestividade do Suporte Técnico:** Em ambiente de cibersegurança, a resolução célere de incidentes é fundamental para mitigar riscos e prevenir potenciais vulnerabilidades. A carta de solidariedade garante o atendimento prioritário de chamados técnicos; o suporte direto do fabricante em casos de complexidade excepcional; o acesso a recursos técnicos especializados; a resolução tempestiva de problemas críticos que possam comprometer a segurança da infraestrutura
- **Garantia de Compatibilidade e Integração:** A diversidade de equipamentos e serviços no ambiente tecnológico demanda soluções com interoperabilidade comprovada; capacidade de integração com sistemas existentes; padronização de protocolos e configurações; e, suporte técnico qualificado para cenários específicos de implementação.
- **Mitigação de Riscos Operacionais:** A carta de solidariedade funciona como mecanismo de redução de riscos de descontinuidade de serviços; garantia de suporte técnico especializado; preservação da eficácia da solução de segurança; minimização de impactos em caso de falhas ou necessidade de atualizações.
- **Alinhamento com Boas Práticas de Governança de TI:** A exigência está alinhada com recomendações de órgãos de controle; melhores práticas internacionais de gestão de infraestrutura de TI; princípios de segurança da informação; e, requisitos de resiliência tecnológica.

Subcontratação

Não é admitida a subcontratação do objeto contratual.

Da verificação de amostra do objeto

Considerando que o item 1 consiste de apenas 2 unidades, não será exigida amostra do objeto.

Garantia da Contratação

Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5 (cinco) % do valor contratual, conforme regras previstas no contrato.

A garantia nas modalidades caução e fiança bancárias deverá prestada em até 5 (cinco) dias após a assinatura do contrato.

Da verificação de amostra do objeto,

Não se aplica.

8. Estimativa da demanda - quantidade de bens e serviços

Abaixo segue o detalhamento da quantidade de bens e serviços necessários à execução do objeto, a saber:

Grupo	Id	Descrição	Quant.	Unid.
	1	Appliance de Firewall de próxima geração (NGFW)	2	Unid.
	2	Console de gerenciamento de logs, análises e relatórios de ameaças de redes (SaaS)	1	Unid.

1	3	Serviços de Instalação e Configuração de Firewall de Próxima Geração	1	Unid.
	4	Treinamento técnico especializado na solução de NGFW (uma turma)	1	Unid.
	5	Operação assistida especializada prestada pelo fornecedor (HST)	500	HST

9. Sobre o item 5 (operação assistida)

Detalhamento técnico,

As atividades de operação assistida serão acionadas em situações que envolvam incidentes críticos ou mudanças significativas na rede da ANM, garantindo suporte especializado para mitigar impactos e assegurar a continuidade operacional. O suporte técnico especializado a ser prestado pelo fornecedor deverá atender às seguintes condições, garantindo alinhamento com as melhores práticas de mercado e a eficiência da solução implantada:

Definição e Disponibilidade do Serviço Técnico,

- O suporte será medido em Horas de Serviço Técnico (HST), com registro detalhado do tempo despendido para cada atividade, desde a abertura da solicitação até sua conclusão. O fornecedor deverá disponibilizar suporte remoto e presencial, conforme a necessidade do cliente.
- Todas as ações deste item serão solicitadas por meio de chamados ou ordens de serviço, conforme a forma mais simples e eficiente acordada entre a CONTRATANTE e a CONTRATADA.

Especialização Técnica,

- A equipe de suporte deverá ser composta por profissionais certificados e capacitados nas tecnologias fornecidas, incluindo as versões e atualizações mais recentes.

Registro e Transparência,

- Cada atendimento deverá ser documentado, incluindo descrição detalhada da solicitação, ações tomadas, tempo de execução e a validação do cliente sobre a conclusão do serviço. O relatório deverá estar disponível para consulta pelo contratante.

Atualizações e Melhoria Contínua,

- Durante o suporte, o fornecedor deverá, quando necessário, aplicar atualizações de software, patches de segurança e recomendações para aprimorar o desempenho ou a segurança da solução.

Garantia de Atendimento Fora do Expediente,

- O suporte deverá estar disponível 24/7 para solicitações emergenciais que impactem a continuidade dos serviços críticos.

Consumo e Acompanhamento,

- O controle do consumo de horas de serviço técnico (HST) será realizado com base em ordens de serviço detalhadas, onde o escopo e o quantitativo de HST necessários serão previamente ajustados. Esse processo assegura que as horas contratadas sejam alocadas de forma eficiente, alinhadas às necessidades específicas de cada atividade demandada, proporcionando flexibilidade e gestão eficaz dos recursos durante a execução dos serviços.

Transferência de Conhecimento,

- Sempre que demandado, o fornecedor deverá realizar ações de Transferência de Conhecimento relacionadas às demandas atendidas, garantindo o fortalecimento da autonomia da equipe do contratante.

Dimensionamento do volume de HST,

A previsão de 500 horas de serviço técnico (HST) para a operação assistida da solução de firewall baseia-se em estimativa elaborada pela área técnica da ANM, considerando a experiência prática acumulada na gestão do firewall atualmente em uso. Trata-se, no entanto, de um serviço inédito no escopo de contratações da Agência, uma vez que o contrato de firewall já encerrado não contou com apoio técnico especializado de operação assistida. Diante disso, não há base histórica consolidada para um benchmark preciso entre a estimativa e o consumo real dessas horas. Assim, o quantitativo estabelecido reflete uma projeção técnica prudencial, podendo ser reavaliado em futuras contratações com base na experiência adquirida durante a execução contratual proposta.

Justificativa da utilização das Horas de Serviço Técnico (HST),

A adoção da métrica de Horas de Serviço Técnico (HST) no item 5 desta contratação está plenamente justificada, considerando sua relevância para a execução eficiente e completa da solução. Essa métrica, amplamente utilizada no segmento de TI, oferece uma abordagem racional e econômica para a Administração, pois permite o acionamento dos serviços de forma pontual e sob demanda, exclusivamente em situações nas quais o time interno de infraestrutura não disponha da expertise necessária para solucionar problemas técnicos específicos da solução contratada.

Além disso, a utilização de HST garante que as demandas estejam vinculadas a critérios claros e objetivos, incluindo prazos previamente definidos, escopo delimitado, produtos específicos a serem entregues, padrões rigorosos de recebimento e aceite, além de acordos de níveis de serviço (SLA) detalhados no edital. Essas condições asseguram que a Administração tenha pleno controle sobre a qualidade e a efetividade das entregas realizadas.

Por fim, essa modalidade é comprovadamente a mais vantajosa e econômica para esse tipo de serviço (operação assistida), pois evita a contratação contínua de serviços não necessários, reduzindo custos e otimizando recursos públicos. Assim, a utilização de HST atende integralmente às diretrizes da Portaria nº 94/2022, garantindo alinhamento com as melhores práticas do setor e promovendo eficiência e economicidade na gestão dos serviços contratados.

Consumo das HST,

O consumo desse total de HST será controlado da seguinte forma:

Demandas Pontuais:

- O controle será realizado por meio da abertura de chamados específicos.
- Cada chamado deverá registrar a data e hora de abertura, a data e hora de encerramento e o grau de severidade da demanda.
- Independentemente do grau de severidade atribuído ao chamado, será contabilizado o consumo fixo de 3 (três) horas de HST por atendimento.

Essa definição se justifica pelo fato de que, mesmo em chamados críticos, o atendimento deverá ocorrer no prazo de até 3 horas, e em chamados de severidade menor, embora o prazo de resolução seja maior, o tempo efetivo de atendimento típico é compatível com esse limite de 3 horas.

Demandas Estruturadas:

- O controle será feito mediante a emissão de Ordem de Serviço (OS).
- Cada OS deverá conter o escopo detalhado da atividade e a estimativa de horas necessárias para sua execução.
- As horas consumidas serão registradas e consolidadas em relatórios mensais, que deverão comprovar o uso das horas, sob pena de glosa em caso de não comprovação.

10. Levantamento de soluções

Alternativa 1: Aquisição de um Firewall de Próxima Geração (NGFW)

A alternativa 1 consiste na aquisição de uma solução completa de Firewall de Próxima Geração (NGFW) para substituir o equipamento atual da ANM, que encontrase sem suporte e atualização. Essa abordagem visa atender às necessidades de proteção avançada da infraestrutura de TI da organização, garantindo maior segurança cibernética, desempenho e conformidade regulatória. O NGFW proposto oferece as seguintes capacidades principais:

- **Proteção Avançada contra Ameaças:** Combate a ataques sofisticados, como malware, ransomware e tentativas de intrusão, com recursos como IPS (Intrusion Prevention System), análise de tráfego criptografado (SSL/TLS) e controle granular de aplicações.

- Conformidade Regulamentar: Garantia de aderência a normas e regulamentações, como a Lei Geral de Proteção de Dados (LGPD), com proteção adequada aos dados sensíveis e críticos.
- Escalabilidade e Desempenho: Solução projetada para crescer com as demandas do órgão, suportando aumento no volume de tráfego, usuários e dispositivos sem comprometer a performance.
- Centralização e Gestão Simplificada: Facilita a administração das políticas de segurança, com monitoramento centralizado e interfaces intuitivas para reduzir a complexidade operacional.
- Resiliência e Continuidade de Operações: Responde rapidamente a falhas e ataques, minimizando impactos às operações críticas.

Essa alternativa é a mais alinhada ao cenário atual da ANM, que enfrenta ameaças cibernéticas crescentes e depende de um ambiente protegido para assegurar a confidencialidade, integridade e disponibilidade de suas informações e serviços. Além disso, o NGFW possibilitará a modernização da infraestrutura de segurança de TI, reduzindo riscos operacionais e melhorando a eficiência no combate a ameaças.

Alternativa 2: Contratação de Firewall como Serviço (FaaS)

A alternativa 2 propõe a contratação de um Firewall de Próxima Geração (NGFW) como serviço (FaaS). Nesse modelo, a ANM não adquire diretamente o equipamento, mas sim um serviço completo gerido por um fornecedor especializado, que inclui o fornecimento, manutenção e operação do firewall. Os principais aspectos dessa alternativa são:

- Modelo de Serviço: O fornecedor é responsável por implementar, gerenciar e manter o NGFW, incluindo atualizações, suporte técnico e configuração contínua, conforme as necessidades da ANM.
- Benefícios de Custo: Redução do investimento inicial em hardware e licenças, com o pagamento realizado em modelo de assinatura ou por uso, o que facilita a gestão financeira.
- Atualizações Contínuas: Garantia de que o firewall estará sempre atualizado contra as ameaças mais recentes, sem depender de ações da ANM para realizar upgrades ou aplicar patches.
- Flexibilidade e Escalabilidade: Permite ajustes rápidos na capacidade ou recursos do firewall, de acordo com a evolução das necessidades da agência.
- Foco na Operação: A equipe interna da ANM pode concentrar esforços em outras atividades estratégicas, deixando a gestão da segurança perimetral a cargo do fornecedor.

Essa alternativa é ideal para organizações que desejam acesso a tecnologias avançadas de segurança sem a complexidade de gestão interna ou os custos elevados de aquisição e manutenção direta. O modelo FaaS traz eficiência operacional, segurança robusta e conformidade contínua, além de se adaptar bem a ambientes dinâmicos.

Alternativa 3: Contratação de Garantia Estendida para o Firewall Atual

A alternativa 3 propõe a manutenção dos equipamentos e softwares de firewall atualmente em uso na ANM, por meio da contratação de uma garantia estendida para os appliances Fortigate 1500D atualmente em operação. Esses equipamentos possuem previsão de fim de vida útil (End of Support - EOS) estabelecida pela Fortinet até dezembro de 2026. Essa abordagem busca assegurar a continuidade do suporte técnico e das atualizações necessárias durante um período adicional, garantindo a operacionalidade e a segurança da solução. Os principais aspectos dessa alternativa incluem:

- Continuidade com o Firewall Existente: Permite que a ANM continue utilizando o hardware e o software já implantados, prolongando sua vida útil.
- Cobertura de Suporte Técnico: A garantia estendida garantiria suporte técnico para resolução de falhas e problemas operacionais, além de acesso a atualizações de segurança críticas e correções de vulnerabilidades.
- Menor Investimento Inicial: Essa alternativa requer menor investimento financeiro em comparação à aquisição de novos equipamentos, representando uma solução econômica a curto prazo.
- Limitações Técnicas: Embora viável, essa alternativa não resolve problemas estruturais ou de obsolescência do firewall atual, que pode não acompanhar as necessidades de segurança cibernética e escalabilidade da ANM a médio e longo prazo.

A contratação de uma garantia estendida é uma solução temporária que busca mitigar riscos imediatos de vulnerabilidades e falhas, enquanto preserva recursos financeiros. Contudo, é importante frisar que o firewall atual possivelmente não atenderá às demandas futuras da organização.

11. Análise comparativa de soluções

A seguir, é apresentada uma análise comparativa entre as três alternativas propostas para atender às necessidades de segurança da rede da ANM, considerando fatores técnicos, operacionais e estratégicos:

Alternativa 1: Aquisição de um Firewall de Próxima Geração (NGFW)

Características principais: O firewall adquirido torna-se patrimônio da ANM, eliminando custos fixos anuais para pagamento de serviços após a aquisição. Garantia de 60 meses assegura atualizações de software, suporte técnico, e continuidade operacional. Permite que a ANM mantenha um controle total sobre a solução, estando em conformidade com a prática mais comum na administração pública. A solução tem maior previsibilidade orçamentária, já que os custos são concentrados na aquisição inicial.

Vantagens:

- Custo-benefício em longo prazo por evitar despesas recorrentes anuais.
- Maior independência operacional e flexibilidade no gerenciamento da solução.
- Alinhamento com práticas consolidadas no setor público.

Desvantagens:

- Requer investimento inicial mais elevado.
- Responsabilidade pela manutenção da infraestrutura cabe à ANM.

Alternativa 2: Contratação de Firewall como Serviço (FaaS)

Características principais: O firewall é oferecido como um serviço gerenciado na nuvem, eliminando a necessidade de aquisição de hardware ou licenças de software. Demanda orçamento anual para a manutenção do serviço, cobrindo atualizações, suporte técnico e infraestrutura. É uma prática mais comum na iniciativa privada, com pouca aplicação consolidada na administração pública, no caso em tela obtivemos uma proposta da TELEBRAS para fornecimento dessa solução como serviço (documento16266202).

Vantagens:

- Redução da complexidade de gerenciamento, com a responsabilidade técnica delegada ao fornecedor.
- Escalabilidade e flexibilidade, permitindo adaptações rápidas às necessidades da ANM.
- Atualizações e suporte são garantidos continuamente pelo fornecedor.

Desvantagens:

- Dependência orçamentária anual, representando um risco, especialmente diante de incertezas fiscais no setor público.
- Pode ser mais custoso em longo prazo, dependendo das condições contratuais.
- Pouco utilizado na administração pública, tornando sua contratação mais complexa.

Alternativa 3: Contratação de Garantia Estendida para o Firewall Existente

Características principais: A alternativa 3 consiste na contratação de uma extensão de garantia e suporte técnico para o firewall atualmente em uso pela ANM, cujo equipamento já se encontra fora de suporte e licenciamento desde o início de 2024. Apesar de representar uma solução economicamente atraente no curto prazo, essa alternativa enfrenta restrições significativas devido à proximidade do fim da vida útil (EOS) do equipamento, prevista pela fabricante para dezembro de 2026, e à dificuldade de encontrar fornecedores dispostos a oferecer suporte para equipamentos com mais de 5 anos de uso.

Vantagens:

- Custo inicial reduzido: Evita a necessidade de aquisição imediata de novos equipamentos, gerando economia no curto prazo.
- Prolonga a vida útil do ativo: Maximiza o uso do equipamento atual, retardando o investimento em substituições.

Desvantagens:

- Risco operacional elevado: O equipamento encontra-se desatualizado, com tecnologias e recursos de segurança inferiores aos modelos atuais.

- Limitação tecnológica: O desempenho reduzido e a ausência de funcionalidades modernas podem impactar negativamente a eficiência e a segurança das operações.
- Falta de suporte pleno: A ausência de garantia original e suporte adequado compromete a cibersegurança, a continuidade operacional e aumenta a vulnerabilidade frente às crescentes ameaças cibernéticas.
- Custo processual: Uma contratação desse tipo apenas posterga a solução do problema do firewall (até dezembro de 2026), e não resolve o modelo de execução da solução (pois não prevê, modernização dos serviços demandados e nem operação assitida).

Considerações Finais:

- A Alternativa 1 (Aquisição de um NGFW) destaca-se como a mais segura e viável em termos de investimento a longo prazo, previsibilidade orçamentária e controle operacional.
- A Alternativa 2 (FaaS) pode ser considerada inovadora, mas apresenta riscos devido à dependência de orçamento contínuo e menor adoção no setor público.
- A Alternativa 3 (Garantia Estendida), embora econômica, apresenta riscos elevados e limitações que podem comprometer as operações e a segurança da ANM. Essa alternativa, apesar de parecer vantajosa do ponto de vista econômico inicial, apresenta riscos consideráveis que podem impactar diretamente a segurança e a eficiência das operações da Agência no médio prazo.

12. Registro de soluções consideradas inviáveis

Após análise detalhada das alternativas para a solução de firewall da ANM, identificaram-se limitações que tornam as Alternativas 2 e 3 inviáveis para atender às necessidades da organização de forma segura e eficiente, a saber:

Alternativa 2: Contratação de Firewall como Serviço (FaaS)

Embora o modelo FaaS seja tecnicamente viável e amplamente utilizado na iniciativa privada, ele apresenta desafios significativos no contexto da administração pública, que comprometem sua implementação na ANM:

- Dependência Orçamentária Contínua: Este modelo exige orçamento anual para pagamento do serviço, o que representa um risco elevado em virtude da imprevisibilidade de alocações orçamentárias no setor público. A descontinuidade do serviço por falta de pagamento comprometeria diretamente a segurança cibernética da ANM.
- Falta de Experiência no Setor Público: Não foi possível identificar contratos em vigência no setor público que utilizem este modelo. A ausência de experiências similares eleva o risco de entraves legais, contratuais e operacionais durante a implementação e gestão do serviço.
- Custo em Longo Prazo: Embora o FaaS elimine a necessidade de aquisição de hardware, os custos recorrentes ao longo dos anos tendem a ser mais altos que a aquisição de um NGFW como ativo.

Conclusão: A falta de previsibilidade orçamentária e de referências na administração pública tornam o modelo FaaS impraticável para a ANM no momento.

Alternativa 3: Garantia Estendida para o Firewall Existente

A alternativa de estender a garantia do equipamento atual também apresenta sérias limitações que a tornam inviável:

- Obsolescência do Equipamento: O firewall atual tem mais de 5 anos de uso, o que o classifica como tecnologicamente obsoleto. Este equipamento não suporta as demandas de segurança cibernética modernas, como proteção contra ameaças avançadas e desempenho adequado para o ambiente atual da ANM.
- Inexistência de Garantia Estendida Viável: Não foi possível identificar fornecedores que ofereçam garantia estendida para um firewall desse porte e com idade avançada. Além disso, eventuais soluções disponíveis podem ser limitadas em escopo e cobertura, não garantindo o mesmo nível de proteção de um equipamento novo.
- Risco Elevado à Segurança: A dependência de um equipamento desatualizado e sem suporte contínuo coloca a ANM em alto risco de ataques cibernéticos, expondo dados sensíveis e comprometendo a operação dos sistemas.
- Impacto Operacional: Manter um firewall ultrapassado pode resultar em interrupções frequentes, desempenho inadequado e incapacidade de implementar atualizações essenciais, comprometendo a produtividade e a eficiência.
- Custo processual: Uma contratação desse tipo apenas posterga a solução do problema do firewall (até dezembro de 2026), e não resolve o modelo de execução da solução (pois não prevê, modernização dos serviços demandados e nem operação assitida).

Conclusão:

A ausência de suporte adequado para o firewall atual e a impossibilidade de garantir sua segurança e desempenho tornam essa alternativa inadequada para as necessidades críticas da ANM. Com base nos riscos operacionais, estratégicos e orçamentários, conclui-se que as Alternativas 2 (FaaS) e 3 (Garantia Estendida) não atendem aos requisitos de segurança e confiabilidade exigidos pela ANM. Dessa forma, a Alternativa 1 (Aquisição de um NGFW) permanece como a única solução viável, equilibrando custo, previsibilidade orçamentária e garantia de proteção de longo prazo.

13. Análise comparativa de custos (TCO)

Alternativa 1 – Aquisição de um Firewall de Próxima Geração (NGFW):

- **Custo inicial (primeiro ano):** R\$ 2.673.383,88
- **Custo anual subsequente:** R\$ 367.192,78 (do segundo ao quinto ano, sujeito a reajuste)
- **Custo total em 5 anos:** R\$ 4.142.154,00 (estimado, considerando reajustes).

Essa alternativa apresenta o segundo maior investimento inicial, mas os custos anuais subsequentes são significativamente mais baixos, garantindo maior previsibilidade orçamentária e economicidade ao longo do período de 5 anos. Além disso, inclui todos os elementos necessários à implementação e operação da solução, como treinamento, operação assistida e console de gerenciamento.

Alternativa 2 – Contratação de Firewall como Serviço (FaaS):

- **Custo anual fixo:** R\$ 3.013.430,88 (sujeito a reajustes anuais).
- **Custo total em 5 anos:** R\$ 15.067.154,40 (estimado, considerando reajustes).

Embora essa alternativa elimine a necessidade de aquisição inicial de hardware, seu custo anual elevado a torna menos atrativa em termos de custo-benefício ao longo de 5 anos. A ausência de um patrimônio ao final do contrato e a dependência contínua de orçamento também representam desvantagens financeiras e operacionais. Foram considerados os valores da proposta da TELEBRAS para fornecimento dessa solução como serviço (documento 16266202).

Alternativa 3 – Contratação de Garantia Estendida para o Firewall Existente:

- **Custo do primeiro ano:** R\$ 919.555,80
- **Custo do segundo ano:** R\$ 72.353,63
- **Custo total em 2 anos:** R\$ 991.909,43

Essa alternativa tem o menor custo inicial, mas sua validade é limitada a dois anos, devido ao fim da vida útil (EOS) do equipamento em dezembro de 2026. Após esse período, a ANM ainda precisará adquirir uma nova solução, implicando em um novo investimento significativo. Adicionalmente, os riscos operacionais e a falta de suporte completo podem acarretar custos indiretos não previstos.

Resumo Comparativo:

1. **Alternativa 1 (NGFW):** Apresenta o segundo maior investimento inicial, mas se mostra a mais vantajosa em longo prazo, garantindo previsibilidade orçamentária, controle operacional e modernidade tecnológica.
2. **Alternativa 2 (FaaS):** Embora inovadora, é a opção mais onerosa em 5 anos, além de trazer dependência contínua do orçamento e menor adesão no setor público.
3. **Alternativa 3 (Garantia Estendida):** É a opção mais econômica no curto prazo, mas carece de sustentabilidade operacional e não resolve a demanda em longo prazo, necessitando de substituição após dois anos.

Conclusão:

Com base nos custos e riscos envolvidos, a **Alternativa 1** se destaca como a solução mais equilibrada e economicamente viável, considerando a segurança cibernética, a continuidade operacional e a modernização tecnológica da ANM.

14. Estimativa de custo total da contratação

Valor (R\$): 2.673.383,88

Com base no orçamento estimativo (documento 16218603), o valor estimado da contratação da alternativa 1 é detalhado abaixo:

Item	Fonte	Qty.	Valor Unit. Médio	Valor Total
1	Appliance de Firewall de próxima geração (NGFW)	2	R\$ 1.059.002,72	R\$ 2.118.005,44
2	Console de gerenciamento de logs, análises e relatórios de ameaças de redes (SaaS)	1	R\$ 180.884,09	R\$ 180.884,09
3	Serviços de Instalação e Configuração de Firewall de Próxima Geração	1	R\$ 146.577,73	R\$ 146.577,73
4	Treinamento técnico especializado na solução de NGFW (uma turma)	1	R\$ 41.607,93	R\$ 41.607,93
5	Operação assistida especializada prestada pelo fornecedor (HST)	500	R\$ 372,62	R\$ 186.308,69
	Valor total médio			R\$ 2.673.383,88

Com base na metodologia descrita, o valor total estimado para a execução do primeiro ano deste objeto é de **R\$ 2.673.383,88 (dois milhões, seiscentos e setenta e três mil, trezentos e oitenta e três reais e oitenta e oito centavos).**

Também com base na metodologia descrita, o valor total estimado para a execução a partir do segundo ano, que envolveria apenas a execução dos itens 2 e 5, seria de **R\$367.192,78 (Trezentos e sessenta e sete mil, cento e noventa e dois reais e setenta e oito centavos).**

15. Descrição da solução de TIC a ser contratada

Descrição da Solução 1: Aquisição de um Firewall de Próxima Geração (NGFW)

A Solução 1 consiste na aquisição direta de um Firewall de Próxima Geração (NGFW), que se tornará um ativo da ANM. Essa solução é amplamente adotada na administração pública devido à sua previsibilidade financeira e controle total da infraestrutura adquirida. A aquisição garante que a organização obtenha uma tecnologia de ponta, especificamente dimensionada para atender às suas demandas de cibersegurança e escalabilidade.

Características Principais

Propriedade Permanente do Equipamento:

- Após a compra, o firewall passa a integrar os ativos da ANM, eliminando a dependência de provedores externos para sua operação e manutenção.

Garantia Abrangente de Longo Prazo:

- A garantia de 60 meses inclui suporte técnico 24/7, atualizações contínuas de software e cobertura para todos os componentes de hardware e firmware. Isso assegura que o equipamento mantenha seu desempenho e segurança ao longo do tempo.

Funcionalidades Avançadas:

- O NGFW adquirido será dimensionado para atender às necessidades específicas da ANM, incluindo:
- Inspeção profunda de pacotes (DPI) para identificar e bloquear ameaças.
- Prevenção contra ameaças avançadas (APTs e IOCs).
- Segmentação de rede para proteção de dados sensíveis.
- Suporte à LGPD e regulamentações internacionais de proteção de dados.

Escalabilidade e Performance:

- A solução será projetada para suportar o crescimento da organização em dispositivos, usuários e tráfego de rede, garantindo proteção contínua sem perda de desempenho.

Custo Fixo e Previsibilidade:

- Todos os custos relacionados à implementação, suporte e manutenção são concentrados no momento da aquisição, eliminando despesas recorrentes anuais, comuns em modelos de serviço.

Benefícios:

- **Maior Controle e Independência:** A ANM terá total controle sobre a operação do firewall, sem dependência de contratos anuais ou renovações com fornecedores externos.
- **Redução de Riscos:** A aquisição elimina a possibilidade de interrupções no serviço devido a restrições orçamentárias futuras, garantindo a continuidade da proteção.
- **Adequação Tecnológica:** Com uma solução de última geração, a ANM estará protegida contra ameaças emergentes, com atualizações contínuas e suporte técnico qualificado.
- **Conformidade Regulamentar:** O NGFW adquirido atenderá às exigências de segurança cibernética e proteção de dados, como a LGPD, reforçando a postura da ANM em governança de TI.
- **Sustentabilidade:** A possibilidade de atualizar e manter o equipamento ao longo dos 5 anos de garantia amplia sua vida útil, garantindo eficiência operacional e tecnológica.

Essa solução representa a opção mais viável, segura e eficiente, alinhada às melhores práticas do setor público, garantindo a proteção das operações críticas e dados sensíveis da ANM.

16. Justificativa técnica da escolha da solução

Abaixo apresentamos a justificativa técnica para a escolha da "Alternativa 1: Aquisição de um Firewall de Próxima Geração (NGFW)" a saber:

Crescimento da Rede:

- Com a entrada de novos usuários devido a possíveis concursos públicos e o aumento de dispositivos conectados, a solução permitirá escalabilidade sem comprometimento do desempenho.
- O NGFW pode gerenciar volumes crescentes de tráfego, suportar múltiplas VLANs, integrar novas aplicações e oferecer segmentação de rede para isolar serviços sensíveis.

Publicação e Atualização de Aplicações:

- O NGFW suporta ambientes dinâmicos, garantindo a segurança contínua durante publicações e atualizações de aplicações críticas da ANM, protegendo contra falhas e vulnerabilidades.

Custo Fixo e Previsibilidade:

- A aquisição elimina a necessidade de orçamentos recorrentes, comuns em modelos de serviço, mitigando o risco de contingenciamento de recursos que possam comprometer a continuidade de serviços essenciais.
- A solução será adquirida com garantia de 60 meses, cobrindo manutenção e suporte sem custos adicionais.

Eficiência no Uso de Recursos Públicos:

- Ao adquirir um ativo que pertence à ANM, reduz-se a dependência de serviços externos, garantindo uma abordagem mais econômica no longo prazo e promovendo a autonomia operacional da Agência.

Proteção Contra Ameaças Avançadas:

- O uso de um NGFW atualizado garante proteção contra Ameaças Persistentes Avançadas (APTs), ransomware e ataques de dia zero, os quais não podem ser adequadamente enfrentados por firewalls desatualizados.
- A ANM terá acesso às mais recentes tecnologias de segurança, como inspeção profunda de pacotes (DPI), análise comportamental e proteção de dados sensíveis.

Riscos do Firewall Atual Sem Suporte:

- O firewall atualmente em uso na ANM está sem suporte, expondo a organização a vulnerabilidades conhecidas que podem ser exploradas por atacantes.
- Sem atualizações de segurança, há risco elevado de incidentes como roubo de dados, indisponibilidade de serviços e violações de compliance regulatório.

Conformidade Regulamentar:

- O NGFW atenderá aos requisitos da LGPD e outros regulamentos de proteção de dados, evitando sanções legais e preservando a credibilidade institucional.

Resiliência e Continuidade Operacional:

- A solução será resiliente a falhas, com suporte técnico 24/7 e substituição de hardware, garantindo alta disponibilidade e continuidade das operações, mesmo em cenários adversos.

Facilidade de Gestão:

- O NGFW contará com ferramentas de gerenciamento simplificado e centralizado, reduzindo a carga de trabalho da equipe de TI e otimizando o tempo de resposta a incidentes.

A escolha da Alternativa 1 oferece a melhor combinação de escalabilidade, previsibilidade financeira e robustez em cibersegurança, atendendo de forma plena às necessidades estratégicas e operacionais da ANM. Além disso, assegura que a organização estará preparada para enfrentar desafios tecnológicos futuros, protegendo suas informações sensíveis e garantindo a continuidade de suas operações críticas.

17. Justificativa econômica da escolha da solução

A escolha pela **Alternativa 1** como solução para a demanda de segurança cibernética da ANM é justificada por sua viabilidade econômica em longo prazo, aliada à previsibilidade orçamentária e à eficiência operacional.

Embora apresente um investimento inicial elevado (R\$ 2.673.383,88 no primeiro ano), essa solução elimina a necessidade de custos recorrentes anuais elevados, como ocorre nas alternativas de contratação como serviço (FaaS). Após a aquisição, os custos anuais serão reduzidos a R\$ 367.192,78 (sujeitos a reajustes), o que representa uma economia significativa em comparação à Alternativa 2, que possui custo fixo anual de R\$ 3.013.430,88.

Além disso, a solução adquirida torna-se patrimônio da ANM, permitindo maior independência e controle operacional. O modelo adotado prevê a garantia de 60 meses, incluindo atualizações de software, suporte técnico e manutenção, assegurando a continuidade e a eficiência dos serviços por cinco anos, sem a necessidade de novos aportes financeiros significativos durante esse período.

Comparativamente, a **Alternativa 2 (FaaS)**, apesar de eliminar a aquisição inicial, apresenta um custo total cinco vezes maior em 5 anos, totalizando aproximadamente R\$ 15.067.154,40. Já a **Alternativa 3 (Garantia Estendida)**, embora inicialmente econômica, é inviável em médio e longo prazo, pois não resolve a demanda de modernização tecnológica, deixa a ANM exposta a riscos de descontinuidade e, após dois anos, exigirá um novo investimento de grande porte para substituição dos equipamentos obsoletos.

Portanto, a **Alternativa 1** não apenas apresenta o melhor custo-benefício a longo prazo, como também assegura a modernização tecnológica necessária para enfrentar os crescentes desafios em segurança cibernética, garantindo a proteção das operações críticas da Agência. A adoção dessa solução representa uma escolha pautada na racionalidade econômica e no alinhamento com o princípio da eficiência tão necessários à Administração Pública.

18. Certificações necessárias

Para garantir a segurança, qualidade e conformidade dos firewalls adquiridos, será exigido que os dispositivos possuam as seguintes certificações: Common Criteria (EAL4+), FIPS 140-2 / 140-3, ICSA Labs Certification, CyberRatings.org Recommended Rating, ISO/IEC 27001, UL 2900-1 e Homologação Anatel. A seguir, essas certificações serão detalhadas e justificadas.

A **certificação Common Criteria (EAL4+)** é amplamente reconhecida como um padrão internacional de avaliação de segurança para dispositivos e sistemas de tecnologia da informação. A exigência dessa certificação para um firewall no Brasil pode ser justificada pelos aspectos abaixo.

A Common Criteria fornece uma análise detalhada e padronizada da confiabilidade e segurança de produtos de TI, avaliando sua resistência contra ataques e vulnerabilidades. Um firewall certificado EAL4+ garante que foi submetido a rigorosos testes de segurança, incluindo aspectos como criptografia, controle de acesso e resiliência a invasões. Isso é essencial para proteger redes corporativas críticas contra ataques cibernéticos cada vez mais sofisticados, como ransomware e ameaças persistentes avançadas (APT).

No Brasil, não há uma certificação nacional específica que ofereça o mesmo nível de garantia técnica para dispositivos de segurança, como firewalls. Enquanto normas como a ISO/IEC 27001 abordam a gestão da segurança da informação, elas não avaliam diretamente a robustez técnica de equipamentos de segurança cibernética. A adoção de um padrão internacional reconhecido, como o Common Criteria, preenche essa lacuna, alinhando o país às melhores práticas globais.

Produtos certificados pelo Common Criteria são validados por laboratórios credenciados, garantindo sua qualidade e conformidade com requisitos de segurança. Além disso, como a certificação é reconhecida internacionalmente, ela assegura que o produto seja compatível com outras soluções de segurança e esteja alinhado aos padrões adotados por parceiros e fornecedores globais.

A exigência de certificação Common Criteria reduz os riscos associados ao uso de dispositivos sem comprovação técnica confiável, como falhas de segurança ou desempenho abaixo do esperado. Para organizações públicas e privadas que lidam com informações sensíveis, como a administração pública brasileira, a adoção de soluções certificadas é essencial para evitar incidentes que possam comprometer a integridade, confidencialidade e disponibilidade dos dados.

A certificação Common Criteria também facilita a conformidade com regulamentações nacionais e internacionais de segurança, como a Lei Geral de Proteção de Dados (LGPD), que exige a adoção de medidas técnicas adequadas para proteger informações pessoais. Além disso, em caso de auditorias, a certificação serve como evidência objetiva da robustez do dispositivo utilizado.

Exigir a certificação EAL4+ para firewalls aumenta a credibilidade do processo de aquisição, assegurando que os recursos públicos ou privados estão sendo investidos em uma solução comprovadamente segura e confiável. Isso também reforça a confiança dos stakeholders internos e externos na segurança do ambiente de TI.

A exigência da **certificação FIPS 140-2 / 140-3** para soluções de firewall no Brasil é essencial para garantir a segurança, confiabilidade e conformidade de dispositivos críticos de cibersegurança. Este padrão, emitido pelo NIST (National Institute of Standards and Technology) dos Estados Unidos, avalia rigorosamente os módulos criptográficos, certificando que atendem aos mais altos requisitos de segurança em criptografia.

Razões para exigir FIPS 140-2 / 140-3:

- **Segurança Criptográfica de Alto Nível:** A certificação assegura que os módulos criptográficos do firewall foram testados para resistir a ataques, garantindo a proteção de dados sensíveis contra acesso não autorizado e violações.
- **Garantia de Qualidade:** Soluções com certificação FIPS passam por testes rigorosos que validam sua eficiência e robustez. Isso reduz o risco de falhas e garante o desempenho esperado em cenários críticos.
- **Ausência de Certificação Similar no Brasil:** O Brasil não possui uma certificação equivalente que avalie detalhadamente os módulos criptográficos. Assim, a exigência do FIPS, reconhecido globalmente, preenche essa lacuna e assegura padrões internacionais de segurança.
- **Mitigação de Riscos Cibernéticos:** No contexto do aumento de ameaças, como ransomware e espionagem cibernética, a certificação FIPS minimiza vulnerabilidades relacionadas a criptografia fraca ou mal implementada, contribuindo para a resiliência cibernética.
- **Confiança e Conformidade Regulatória:** Muitos órgãos internacionais e nacionais demandam conformidade com padrões rigorosos, especialmente em setores financeiros, governamentais e de saúde. Firewalls certificados com FIPS 140-2 ou 140-3 são mais confiáveis e preparados para atender a essas exigências.
- **Relação Custo-Benefício:** Apesar do investimento inicial maior, a certificação reduz custos futuros relacionados a incidentes de segurança, atualizações corretivas ou substituição de equipamentos comprometidos.

A exigência da **certificação ICSA Labs** para soluções de firewall no Brasil é uma medida técnica fundamental para assegurar altos padrões de qualidade, desempenho e segurança em um cenário de cibersegurança cada vez mais desafiador. Emitida pelo renomado ICSA Labs, essa certificação reconhece dispositivos que atendem a rigorosos requisitos funcionais e de segurança, garantindo a eficácia contra ameaças cibernéticas e a confiabilidade operacional. Razões para exigir a Certificação ICSA Labs:

- **Garantia de Qualidade e Segurança:** A certificação avalia critérios abrangentes, como prevenção de invasões, detecção de ameaças e controle de acessos, assegurando que o firewall atenda aos mais elevados padrões de qualidade e eficiência.

Essa validação independente reduz os riscos associados a soluções de baixa qualidade ou com vulnerabilidades desconhecidas.

- **Ausência de Certificação Similar no Brasil:** No Brasil, não há uma certificação equivalente que realize testes tão abrangentes e independentes sobre dispositivos de segurança. Assim, a exigência da Certificação ICSA Labs supre essa lacuna, alinhando o mercado brasileiro aos melhores padrões internacionais.
- **Confiança e Reconhecimento Global:** A Certificação ICSA Labs é amplamente reconhecida no setor de cibersegurança, sendo utilizada como referência por governos, grandes corporações e indústrias regulamentadas. Esse reconhecimento internacional confere credibilidade às soluções adquiridas.
- **Teste e Validação em Cenários Reais:** A certificação inclui testes extensivos em cenários reais de ataque e uso. Isso garante que o firewall seja eficiente não apenas no papel, mas também na prática, proporcionando proteção robusta em redes corporativas críticas.
- **Mitigação de Riscos e Resiliência Cibernética:** A certificação valida a capacidade do firewall de prevenir e mitigar ataques avançados, como malwares, ransomware e ataques DDoS. Essa robustez é essencial para proteger informações sensíveis e assegurar a continuidade operacional.
- **Relevância no Setor Público e Privado:** A crescente dependência de sistemas digitais no Brasil, tanto no setor público quanto privado, exige soluções de segurança que sejam confiáveis e eficazes. A certificação ICSA Labs ajuda a garantir que os firewalls adquiridos estejam à altura dessas demandas.

A **certificação CyberRatings.org Recommended Rating** é uma avaliação importante para a segurança de firewalls, pois ela fornece uma análise independente e abrangente da eficácia de soluções de segurança cibernética. No Brasil, exigir essa certificação para a aquisição de firewalls é fundamental pelas seguintes razões:

- **Garantia de Qualidade e Efetividade:** A certificação CyberRatings.org é concedida com base em testes rigorosos de desempenho e segurança, assegurando que a solução atende aos mais altos padrões de proteção contra ameaças cibernéticas. Isso garante que a solução oferecida seja eficaz e robusta para proteger a infraestrutura de TI da organização contra ataques avançados.
- **Segurança Comprovada:** A certificação assegura que o firewall foi testado e validado para detectar e mitigar ameaças, como malware, ransomware, ataques DDoS, e outras vulnerabilidades comuns em redes corporativas. A presença dessa certificação demonstra que o produto tem um histórico de confiabilidade, o que é essencial em um cenário de segurança crescente e ameaças complexas.
- **Avaliação Independente:** A avaliação feita pela CyberRatings.org é independente de qualquer fornecedor ou fabricante, proporcionando uma visão imparcial sobre a performance do firewall. Isso é crucial para garantir que a escolha da solução seja baseada em resultados objetivos, sem influências externas, e que a empresa esteja adquirindo uma solução de segurança realmente eficaz.
- **Adequação ao Mercado Global:** A certificação CyberRatings.org é amplamente reconhecida no mercado internacional e, ao exigí-la, a organização se alinha com as melhores práticas globais de cibersegurança. Isso pode ser especialmente relevante em ambientes corporativos que lidam com informações sensíveis ou operam em várias jurisdições, incluindo a necessidade de atender a regulamentações internacionais de segurança de dados.
- **Ausência de Certificação Similar no Brasil:** Atualmente, o Brasil não possui uma certificação similar que aborde de forma tão específica e técnica as necessidades de avaliação de firewalls. Por isso, adotar a CyberRatings.org Recommended Rating é uma maneira eficaz de garantir que a solução escolhida esteja alinhada com as melhores práticas internacionais, preenchendo uma lacuna importante no mercado local.

A **certificação ISO/IEC 27001** é um padrão globalmente reconhecido que assegura a implementação de controles e processos robustos para a segurança da informação. Sua exigência para firewalls no Brasil é fundamental para garantir que o equipamento atenda a padrões rigorosos de proteção contra ameaças cibernéticas e mitigue riscos de invasões ou vazamentos de dados. Dado que não há certificações nacionais equivalentes que ofereçam a mesma abrangência e padronização, a ISO/IEC 27001 se torna essencial como referência de qualidade e conformidade com boas práticas internacionais. Além disso, sua adoção reforça a confiança em soluções críticas, garantindo que a gestão de segurança segue padrões comprovados e alinhados com exigências legais, como a LGPD.

A **certificação UL 2900-1** é fundamental para garantir a segurança cibernética de dispositivos de rede, como firewalls, ao longo de seu ciclo de vida, desde a concepção até a desativação. Para o Brasil, exigir esta certificação traz diversas vantagens cruciais:

- **Segurança Comprovada:** A UL 2900-1 garante que o firewall tenha sido rigorosamente testado contra vulnerabilidades e que esteja protegido contra falhas de segurança comuns. Isso reduz o risco de ataques cibernéticos que poderiam comprometer dados sensíveis ou a infraestrutura da organização. A certificação assegura que o dispositivo está em conformidade com altos padrões de segurança, promovendo a proteção contínua da rede corporativa.
- **Ausência de Certificação Similar:** No Brasil, embora haja várias certificações de segurança, como ISO/IEC 27001 ou FIPS 140-2, a UL 2900-1 foca especificamente na segurança cibernética dos dispositivos de rede e seu comportamento frente a ameaças emergentes, algo que não é coberto amplamente por outras certificações. Sua exigência garante uma camada adicional de segurança, muitas vezes não oferecida por outros processos de certificação.

- **Garantia de Qualidade e Confiabilidade:** Ao exigir a UL 2900-1, a organização assegura que está adquirindo um produto que passou por testes de resistência a vulnerabilidades de segurança e falhas críticas. Isso resulta em maior confiabilidade, com o firewall oferecendo uma proteção robusta contra ameaças cibernéticas durante seu ciclo de vida, minimizando o risco de falhas operacionais e comprometimento da rede.
- **Adequação a Regulamentações e Conformidade:** Considerando a crescente exigência de conformidade com regulamentações de segurança de dados, como a LGPD (Lei Geral de Proteção de Dados) e outras normas de proteção de dados, a certificação UL 2900-1 pode ser vista como um diferencial competitivo e um compromisso com as boas práticas de segurança. Ela assegura que o dispositivo esteja em conformidade com as exigências internacionais, aumentando a confiança nas operações e diminuindo o risco de penalidades devido a falhas de segurança.

A **homologação da Anatel (Agência Nacional de Telecomunicações)** para dispositivos de telecomunicações e redes, incluindo firewalls, é uma exigência fundamental para garantir que os equipamentos atendam aos requisitos técnicos e de segurança estipulados pelas regulamentações nacionais. A Resolução nº 242 (ou qualquer regulamentação subsequente) estabelece as normas que devem ser seguidas para que o equipamento tenha permissão para operar no Brasil, assegurando a sua conformidade com padrões que garantem tanto o bom funcionamento quanto a proteção de dados e da infraestrutura da rede. Justificativas para a exigência de certificação Anatel para firewalls no Brasil:

- **Segurança e Conformidade Regulatória:** A homologação da Anatel assegura que o dispositivo está em conformidade com as regulamentações brasileiras de segurança cibernética e telecomunicações, conforme as normativas vigentes. A certificação assegura que o firewall não interfere na rede pública de telecomunicações e cumpre com os requisitos de qualidade e segurança.
- **Garantia de Qualidade:** A homologação Anatel atesta que o firewall foi testado e aprovado para operar de acordo com os padrões exigidos, incluindo a conformidade com normas de interferência eletromagnética, desempenho e segurança. Isso significa que o produto foi analisado para garantir que sua operação não cause danos à rede e que atenda aos requisitos de qualidade exigidos pela legislação brasileira.
- **Compatibilidade com a Infraestrutura Nacional:** A certificação garante que o dispositivo, no caso o firewall, seja compatível com as tecnologias e a infraestrutura de telecomunicações brasileiras. Como a Anatel regula o espectro e a implementação de dispositivos de telecomunicações, a homologação assegura que o equipamento funcione de forma eficiente e sem causar problemas de interoperabilidade.
- **Exigências de Mercado e Confiabilidade:** A certificação da Anatel proporciona uma garantia adicional de que o dispositivo está conforme os padrões técnicos exigidos no Brasil. Isso aumenta a confiança dos consumidores e empresas ao adquirirem dispositivos homologados, sabendo que eles atendem às exigências do governo e são aptos para o mercado local, sem comprometer a performance ou a segurança.
- **Prevenção de Riscos Legais:** A falta de homologação Anatel para equipamentos de rede, incluindo firewalls, pode resultar em multas e em problemas legais para a organização, caso o dispositivo não esteja em conformidade com as regulamentações. Exigir essa certificação, portanto, ajuda a minimizar os riscos legais associados ao uso de equipamentos não homologados.

19. Justificativa para a adoção do SRP

O Decreto nº 11.462, de 31 de março de 2023 estabelece as condições para a adoção do Sistema de Registro de Preços (SRP) na Administração, a saber:

"Art. 3º O SRP poderá ser adotado quando a Administração julgar pertinente, em especial:

I - quando, pelas características do objeto, houver necessidade de contratações permanentes ou frequentes;

II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, como quantidade de horas de serviço, postos de trabalho ou em regime de tarefa;

III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas;

IV - quando for atender a execução descentralizada de programa ou projeto federal, por meio de compra nacional ou da adesão de que trata o § 2º do art. 32; ou

V - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

..." (grifos nossos)

A adoção do Sistema de Registro de Preços (SRP) para a presente contratação mostra-se adequada e vantajosa, conforme previsão do art. 3º, incisos II e V, do Decreto nº 11.462/2023. O objeto contempla a contratação de serviços de operação assistida, cuja remuneração se dará por unidade de medida (horas de serviço técnico - HST), característica que se enquadra no inciso II. Além disso, trata-se de um serviço inédito na Agência Nacional de Mineração (ANM), não havendo histórico de consumo que permita estabelecer, com precisão, o quantitativo total a ser demandado, o que caracteriza a situação prevista no

inciso V. A estimativa de 500 horas foi definida com base na experiência da equipe técnica com a gestão do ambiente atual de firewall, mas poderá ser reavaliada durante a vigência do contrato, a depender da efetiva necessidade e da complexidade das atividades envolvidas. Dessa forma, o SRP permite à Administração manter a flexibilidade necessária para atender à demanda de forma eficiente, segura e economicamente vantajosa, sem comprometer a legalidade e a previsibilidade contratual.

20. Benefícios a serem alcançados com a contratação

Um firewall em uma rede corporativa funciona como uma barreira de proteção entre a organização e possíveis ameaças vindas da internet ou de redes internas não confiáveis. Ele monitora, controla e filtra o tráfego de dados, bloqueando acessos não autorizados e ataques cibernéticos. Isso é essencial para proteger informações sensíveis (como dados de usuários e documentos estratégicos da Agência) evitando roubos ou vazamentos, garantir a continuidade dos serviços prevenindo ataques que podem interromper operações críticas, e evitar prejuízos financeiros e danos à reputação reduzindo o risco de violações de segurança que possam gerar multas ou perda de confiança.

Em resumo, o firewall é uma medida indispensável para manter a rede segura, garantindo que as operações fluam sem interrupções e protegendo a empresa contra ameaças cibernéticas cada vez mais sofisticadas. Manter um firewall desatualizado em ambientes corporativos (como o da ANM) apresenta diversos riscos significativos que podem comprometer a segurança e a integridade dos sistemas da organização. Eis alguns desses riscos:

- **Vulnerabilidades Exploits:** Firewalls desatualizados podem conter vulnerabilidades conhecidas que os cibercriminosos podem explorar para acessar a rede corporativa. Sem correções ou patches de segurança, a empresa fica exposta a ataques de exploração que podem resultar em roubo de dados, interrupção dos serviços ou comprometimento da infraestrutura de TI.
- **Falhas de Segurança:** Firewalls desatualizados podem não ser capazes de detectar ou bloquear novas ameaças cibernéticas, como malware avançado, ransomware ou ataques de dia zero. Isso deixa a rede corporativa suscetível a invasões e comprometimentos, colocando em risco informações confidenciais e a reputação da empresa.
- **Compliance e Regulamentação:** Manter um firewall desatualizado pode resultar em não conformidade com regulamentações de segurança cibernética, como o GDPR, HIPAA ou PCIDSS. Isso pode levar a multas significativas e danos à reputação da empresa, especialmente se ocorrer uma violação de dados devido à falta de proteção adequada.
- **Perda de Funcionalidades:** Firewalls desatualizados podem não suportar as últimas tecnologias e recursos necessários para proteger a rede corporativa contra ameaças emergentes. Isso limita a capacidade da empresa de implementar medidas de segurança avançadas, como inspeção SSL, filtragem de conteúdo ou detecção de intrusões avançadas.
- **Desempenho Inferior:** Firewalls desatualizados podem apresentar desempenho inferior devido à falta de otimizações e melhorias de desempenho. Isso pode resultar em latência na rede, tempo de inatividade não planejado e interrupções nos processos de negócios, afetando a produtividade e a eficiência operacional.

Além dos riscos mitigados pela aquisição de um NGFW atualizado e com suporte, essa contratação trará uma série de benefícios estratégicos e operacionais para a ANM. Destacam-se os seguintes pontos complementares:

Benefícios Diretos da Contratação

- **Mitigação de Riscos Cibernéticos Avançados:** A solução oferecerá proteção contra uma ampla gama de ameaças, incluindo ransomware, ataques de dia zero e invasões baseadas em inteligência artificial, garantindo a continuidade das operações e a proteção dos dados da agência.
- **Compliance com Regulamentações:** O novo NGFW permitirá a conformidade com regulamentações locais, como a LGPD, e padrões internacionais, como PCIDSS, reforçando a governança e evitando penalidades financeiras.
- **Aprimoramento da Resiliência Operacional:** A inclusão de funcionalidades como alta disponibilidade (HA) e prevenção de intrusões (IPS) assegurará a continuidade das operações, mesmo em cenários adversos.

Benefícios Estratégicos

- **Modernização Tecnológica:** O investimento em uma solução de última geração posiciona a ANM como uma agência moderna e alinhada às melhores práticas de segurança cibernética, melhorando a confiança dos usuários internos e externos.
- **Melhoria na Experiência dos Usuários:** O desempenho aprimorado da rede garantirá maior eficiência no acesso e na utilização de sistemas corporativos, impactando positivamente a produtividade dos colaboradores e o atendimento ao público.
- **Capacidade de Escalabilidade:** Com a possibilidade de crescimento para suportar demandas futuras, a ANM poderá expandir suas operações sem comprometer a segurança ou o desempenho da infraestrutura.
- **Impactos Adicionais**

- Economia a Longo Prazo: A redução de incidentes de segurança e a prevenção de possíveis violações de dados evitarão custos com recuperação, multas regulatórias e danos à reputação.
- Centralização e Eficiência Operacional: Ferramentas simplificadas de gestão e automação proporcionam uma administração de segurança centralizada, reduzindo a carga de trabalho das equipes de TI.
- Com esses benefícios, a ANM não apenas protegerá sua infraestrutura atual, mas também estará preparada para enfrentar os desafios futuros do ambiente digital, consolidando sua missão de oferecer um serviço público confiável e seguro.

21. Providências a serem Adotadas

Entrega e "moving" dos Equipamentos

Para a entrega dos appliances previstos no Item 1, a contratada deverá realizar a entrega inicial no datacenter da ANM, localizado nas dependências do SERPRO, em Brasília/DF. Após essa entrega, deverão ser executadas as atividades previstas no Item 3, referentes à instalação e configuração dos equipamentos. Concluída essa etapa, a equipe designada pela CONTRATANTE realizará os testes de conformidade. Sendo os resultados satisfatórios, será emitido o termo de recebimento provisório dos bens, seguido do processo de patrimonialização. Posteriormente, ocorrerá a emissão do termo de recebimento definitivo, o respectivo ateste e o pagamento. É de inteira responsabilidade da contratada garantir o transporte seguro ("moving") dos equipamentos até o local indicado, devendo adotar todas as providências necessárias para assegurar que o deslocamento ocorra de forma segura e sem intercorrências.

Recebimento e Validação dos Equipamentos

- Receber os appliances do firewall no local designado.
- Realizar a inspeção física e funcional para verificar conformidade com as especificações técnicas do contrato.
- Emitir Termo de Recebimento Provisório (TRP).

Análise do Firewall Atual

- Avaliar as configurações do firewall atualmente em operação.
- Identificar políticas de segurança, regras, NATs, VPNs e outros elementos essenciais a serem migrados.
- Mapear potenciais vulnerabilidades e ajustes necessários para a migração.

Planejamento da Migração

- Elaborar um plano de migração detalhado para minimizar interrupções, incluindo:
 - Cronograma detalhado.
 - Janelas de manutenção para execução de etapas críticas.
 - Alocar equipes técnicas responsáveis pela implementação e contingências.

Adequação do Ambiente

- Verificar infraestrutura física e lógica necessária:
 - Espaço no rack.
 - Capacidade de energia e redundância.
 - Cabeamento estruturado.
 - Compatibilidade com outros dispositivos de rede.
- Atualizar ou ajustar sistemas dependentes, como servidores de autenticação e monitoramento.
- Instalação e Configuração Inicial
- Instalar fisicamente o novo NGFW na rede.
- Realizar a configuração básica, como endereçamento IP, integração com servidores (LDAP, RADIUS) e conectividade com sistemas dependentes.

Migração das Configurações

- Migrar gradualmente as configurações do firewall atual para o novo NGFW.
- Implementar regras, políticas e integrações críticas, como VPNs, WAF e IPS.
- Testar e validar cada configuração migrada.

Testes Operacionais

- Realizar testes de conectividade e desempenho para garantir funcionamento adequado.
- Simular cenários de ataque para verificar a eficácia das políticas de segurança.
- Ajustar regras e políticas conforme necessário.

Transferência de Conhecimento

- Item 3: Durante a implantação, repasse de informações para a equipe da contratante, apresentando as configurações realizadas, a topologia final e procedimentos executados. Esta transferência de conhecimento deve contemplar minimamente, a documentação completa dos trabalhos e configurações executadas e ao menos 01 (uma) reunião de repasse para a equipe da CONTRATANTE ou time por ela indicado. Documentação Detalhada,
- Item 4: (a) A CONTRATADA deverá indicar um técnico habilitado, com profundo conhecimento na solução NGFW ofertada, para ministrar o treinamento técnico especializado. (b) A capacitação será destinada a uma turma de, no máximo, 10 (dez) técnicos indicados pela CONTRATANTE, abordando, de forma teórica e prática, os procedimentos essenciais de configuração, monitoramento, manutenção e resolução de incidentes, incluindo dentre outras, a migração de regras e a gestão das funcionalidades avançadas da solução. (c) O treinamento deverá ter carga horária de até 48 (quarenta e oito) horas, realizado na modalidade remota (online), com metodologia e conteúdo programático definidos em conjunto com a CONTRATANTE, garantindo a padronização dos processos operacionais e a continuidade da infraestrutura de segurança.
- Item 5: (a) Sempre que demandado, o fornecedor deverá realizar ações de Transferência de Conhecimento relacionadas às demandas atendidas, garantindo o fortalecimento da autonomia da equipe do contratante.
- Demais orientações a cada um dos itens acima descritas no Edital.

Validação Final e Aceitação

- Validar todas as etapas concluídas com base nos critérios de aceitação definidos no contrato.
- Emitir Termo de Recebimento Definitivo (TRD) após a aprovação final.
- Suporte e Operação Assistida
- Garantir período de suporte inicial com operação assistida.
- Resolver dúvidas e ajustar configurações conforme necessidade.

Necessidades de Adequação do Ambiente

Infraestrutura

- Garantir capacidade elétrica e espaço adequado no rack.
- Certificar que a estrutura de rede suporta as capacidades do novo firewall, como VLANs e segmentação.

Equipe

- Disponibilizar pessoal capacitado para participar da migração e operar o novo sistema.
- Organizar cronograma de treinamentos técnicos.

Documentação

- Garantir que a equipe técnica tenha acesso à documentação atualizada do ambiente de TI.
- Produzir e manter registros das configurações realizadas no NGFW.

Sistemas de Apoio

- Atualizar ou adequar servidores de autenticação, como LDAP e RADIUS.
- Integrar o NGFW com sistemas de monitoramento existentes.

Plano de Contingência

- Preparar um plano de rollback em caso de falhas durante a migração.
- Disponibilizar um firewall de backup ou redundante para garantir a continuidade.

22. Declaração de Viabilidade

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

22.1. Justificativa da Viabilidade

Após análise detalhada dos aspectos técnicos, operacionais, de segurança cibernética e orçamentários, declara-se que a Alternativa 1: Aquisição de um Firewall de Próxima Geração (NGFW) é a opção viável e mais adequada para atender às necessidades estratégicas e operacionais da ANM. Seguem os principais fundamentos que suportam essa conclusão:

Aspectos Técnicos

A aquisição do NGFW como ativo proporciona uma solução robusta e escalável, capaz de atender às demandas de segurança cibernética da ANM, considerando:

- Capacidade de Escalabilidade: A solução é preparada para o aumento de usuários, dispositivos e tráfego de rede, especialmente em cenários de expansão, como concursos públicos e novas aplicações.
- Atualizações e Suporte Técnico Garantidos: O contrato inclui suporte técnico contínuo e atualizações automáticas de firmware e software por 60 meses, garantindo que a tecnologia permaneça na vanguarda e capaz de enfrentar ameaças emergentes.
- Proteção Avançada: O NGFW adquirido oferece funcionalidades críticas, como inspeção de tráfego criptografado, análise de comportamento de rede e integração com sistemas de detecção de ameaças, fundamentais para um ambiente seguro.

Mitigação de Riscos

A escolha desta alternativa reduz significativamente os riscos identificados, como:

- Risco de Falhas de Segurança: A substituição do equipamento obsoleto, atualmente sem suporte, elimina as vulnerabilidades associadas à falta de atualizações, prevenindo incidentes cibernéticos graves.
- Continuidade Operacional: A garantia estendida e o suporte técnico asseguram a operação ininterrupta, mesmo em situações de crise, reduzindo o impacto de potenciais incidentes.
- Orçamento Controlado: Por se tratar de um ativo, a solução não gera custos fixos anuais imprevisíveis, mitigando o impacto de contingenciamentos orçamentários.

Benefícios Estratégicos

- Cibersegurança Fortalecida: A implementação de um NGFW moderno alinha a ANM às melhores práticas de segurança digital, protegendo dados sensíveis e aplicações críticas.
- Conformidade com Regulamentações: A solução atende às exigências normativas, reforçando a responsabilidade institucional e evitando sanções legais.
- Eficiência Econômica: A aquisição do equipamento elimina a necessidade de renovação de contratos anuais, oferecendo um excelente custo-benefício a longo prazo.

Comparativo com Outras Alternativas

- A Alternativa 2 (FaaS) apresenta riscos orçamentários significativos devido à necessidade de alocações anuais e à incerteza sobre a continuidade financeira. Além disso, não há referência sólida de adoção desse modelo em órgãos públicos.
- A Alternativa 3 (Garantia Estendida) é inviável, pois não há fornecedores que ofereçam suporte a equipamentos com mais de cinco anos de uso, comprometendo a segurança e a continuidade das operações.

Conclusão

A Alternativa 1 é a única solução tecnicamente viável e estrategicamente alinhada às necessidades da ANM. Ela combina segurança avançada, escalabilidade e previsibilidade orçamentária, garantindo que a Agência esteja equipada para enfrentar os desafios de um cenário cibernético cada vez mais complexo.

23. 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](#).

CLAUDIO PEREIRA

Integrante Requisitante - Líder



Assinou eletronicamente em 29/04/2025 às 15:27:22.

MARCIO JOSE ANTUNES GOMES

Integrante Técnico



Assinou eletronicamente em 29/04/2025 às 15:57:41.

FABIO FERNANDO BORGES

Autoridade competente