

AGENCIA NACIONAL DE MINERAÇÃO - DF

Termo de Referência 144/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
144/2024	323102-AGENCIA NACIONAL DE MINERAÇÃO - DF	CLAUDIO PEREIRA	01/09/2025 13:15 (v 4.1)
Status			
ASSINADO			

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Bens de TIC		48051.000207/2024-91

1. Condições gerais da contratação

1.1. Registro de preços para uma eventual contratação de uma “Solução de Firewall de Próxima Geração (NGFW)” destinada a atender as necessidades da ANM, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento:

Grupo	Id	Descrição	Quant.	Unid.	CATSER CATMAT	Valor Unit.	Valor Total
1	1	Appliance de Firewall de próxima geração (NGFW)	2	Unid.	CATMAT 609340	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	Unid.	CATSER 27502	R\$ 180.884,09	R\$ 180.884,09
	3	Serviços de Instalação e Configuração de Firewall de Próxima Geração	1	Unid.	CATSER 27111	R\$ 146.577,73	R\$ 146.577,73
	4	Treinamento técnico especializado na solução de NGFW (uma turma)	1	Unid.	CATSER 16837	R\$ 41.607,93	R\$ 41.607,93
	5	Operação assistida especializada prestada pelo fornecedor (HST)	500	HST	CATSER 27510	R\$ 372,62	R\$ 186.308,69
Total							R\$ 2.673.383,88

- 1.2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.
- 1.3. Os bens, item 1 do objeto desta contratação são caracterizados como comuns. O serviço a ser contratado é considerado como um serviço comum de acordo com a Lei de Licitações. Os serviços comuns referem-se a atividades rotineiras e amplamente disponíveis no mercado, que não exigem especificações técnicas complexas ou personalização significativa. São serviços que podem ser padronizados e realizados de forma relativamente simples. Nesse contexto, o serviço em questão se enquadra nessa categoria, uma vez que não apresenta características extraordinárias ou particularidades que demandem uma abordagem especializada.
- 1.4. O prazo de vigência da contratação é de 1 (um) ano contados da assinatura do contrato, prorrogável para até 5 (cinco) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.
- 1.4.1 Os serviços prestados por meio dos itens 2 e 5 são enquadrados como continuados tendo em vista a necessidade constante de monitoramento, análise e suporte técnico para garantir a segurança e eficiência da infraestrutura de rede, portanto, a continuidade desses serviços é essencial para manter a proteção contra ameaças cibernéticas, assegurar a operação ininterrupta dos sistemas e proporcionar suporte técnico especializado, garantindo assim a integridade e disponibilidade dos dados e serviços da Agência, sendo a vigência plurianual mais vantajosa considerando o Estudo Técnico Preliminar.
- 1.5. O prazo de execução dos itens 1, 3 e 4 será de 12 (doze) meses contados da assinatura do contrato, não sendo de caráter continuado.
- 1.6. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

## 2. Descrição da solução

- 2.1. A solução de TIC consiste em: (a) equipamentos de firewall de próxima geração (NGFW), (b) console de gerenciamento de logs, análises e relatórios de ameaças de redes (SaaS), (c) serviços de instalação e configuração, (d) treinamento, e (e) serviço especializado de operação assistida.
- 2.2. 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.
- 2.3. 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.
- 2.4. 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.
- 2.5. 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.
- 2.6. 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.
- 2.7. A definição do número de appliances 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.

2.8. 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.

2.9. 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.

2.10. 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.

2.11. 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.

2.12. 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.

2.13. 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.

2.14. 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.

2.15. 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.

2.16. 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.

2.17. 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.

Justificativa: Foi necessário refazer o texto original, uma vez que sua redação apresentava caráter genérico e não refletia com as especificidades técnicas e operacionais do objeto em questão, comprometendo a clareza, a aderência e a efetividade da contratação pretendida.

### 3. Fundamentação e descrição da necessidade

3.1. A ANM deve efetuar esta contratação devido a uma série de razões fundamentais que visam garantir a segurança, eficiência e eficácia de suas operações de rede. Abaixo estão os fundamentos técnicos que destacam a viabilidade e a adequação dessa escolha:

- **Atualização Tecnológica Necessária:** Os firewalls atualmente em uso pela ANM estão desatualizados e fora de suporte, o que os torna suscetíveis a vulnerabilidades e ameaças cibernéticas. A contratação de novos appliances de firewall de próxima geração (NGFW) permitirá à ANM atualizar sua infraestrutura de segurança para uma solução mais moderna e robusta, capaz de lidar com as ameaças emergentes e os requisitos de segurança atuais.
- **Melhoria da Segurança Cibernética:** Com o aumento das ameaças cibernéticas e a sofisticação dos ataques, é essencial que a ANM mantenha uma postura de segurança robusta em sua rede. Os NGFWs oferecem recursos avançados de segurança, como detecção de ameaças em tempo real, prevenção contra intrusões e análise de tráfego avançada, que ajudarão a proteger os ativos e dados da ANM contra ataques maliciosos.
- **Aprimoramento da Eficiência Operacional:** Além de melhorar a segurança, os novos firewalls NGFW também proporcionarão uma maior eficiência operacional. Com recursos avançados de gerenciamento e automação, como console de gerenciamento centralizado e playbooks de resposta a incidentes, a equipe de TI da ANM poderá gerenciar e monitorar a rede de forma mais eficaz, identificar e responder rapidamente a ameaças, e simplificar as operações diárias.
- **Conformidade com as Normas Regulatórias:** Como uma agência governamental, a ANM está sujeita a regulamentações e requisitos de conformidade rigorosos em relação à segurança da informação. A adoção de firewalls NGFW atualizados ajudará a garantir que a ANM esteja em conformidade com as normas e regulamentos relevantes, protegendo assim a integridade e confidencialidade dos dados confiados à agência.
- **Investimento a Longo Prazo:** A contratação de novos firewalls NGFW representa um investimento a longo prazo na segurança e estabilidade da rede da ANM. Essa atualização tecnológica não apenas protegerá a agência contra ameaças atuais, mas também garantirá que ela esteja preparada para enfrentar os desafios de segurança cibernética do futuro, protegendo assim seus ativos e operações de forma contínua e sustentável.
- **Proteção Avançada contra Ameaças:** A adoção de firewalls de próxima geração representa uma resposta eficaz à crescente sofisticação dos ataques cibernéticos. Esses firewalls são projetados para fornecer uma defesa robusta contra ameaças avançadas, como ransomware, utilizando tecnologias avançadas de detecção e prevenção.
- **Adaptabilidade a Ambientes em Evolução:** A ANM está em constante evolução, e os firewalls de próxima geração são capazes de se adaptar dinamicamente a mudanças na infraestrutura. Isso inclui a capacidade de suportar a adição de novos dispositivos, servidores e locais sem comprometer a segurança da rede.
- **Conformidade com Padrões de Segurança:** A escolha de firewalls de próxima geração alinha-se com as melhores práticas de segurança cibernética recomendadas para órgãos governamentais. Isso garante que a ANM mantenha um padrão elevado de segurança e esteja em conformidade com regulamentações específicas do setor público.
- **Monitoramento Avançado e Resposta Rápida a Incidentes:** Os firewalls de próxima geração oferecem recursos avançados de monitoramento, permitindo a detecção precoce de atividades suspeitas na rede. Isso possibilita uma resposta rápida a incidentes, minimizando o tempo de exposição a possíveis ameaças e reduzindo o impacto de ataques.
- **Flexibilidade e Escalabilidade:** Os firewalls de próxima geração são altamente escaláveis e podem ser implantados em diferentes ambientes, incluindo nuvem pública e privada. Isso confere à ANM a flexibilidade necessária para atender às demandas futuras de sua infraestrutura de rede, acompanhando seu crescimento e evolução.
- **Eficiência de Recursos e Minimização de Custos:** A implementação de firewalls de próxima geração proporciona uma abordagem mais eficiente e focada em segurança, reduzindo a necessidade de investimentos massivos em infraestrutura de segurança. Isso minimiza os custos relacionados a incidentes de segurança, como os derivados de ataques cibernéticos, proporcionando economia de recursos e minimização de custos imprevistos.

3.2. Em suma, a justificação técnica para a aquisição da solução de firewall de próxima geração (NGFW) destaca a robustez da solução em enfrentar os desafios específicos da ANM, ao mesmo tempo em que se alinha aos padrões de segurança governamentais e oferece a flexibilidade necessária para um ambiente dinâmico e em expansão. Essa escolha representa um compromisso proativo com a segurança cibernética e a proteção dos ativos digitais da ANM.

#### **Benefícios e resultados esperados,**

3.3. 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.

#### 3.4. A contratação da solução em tela traz diversos benefícios para a ANM e se justifica sobretudo por:

- **Atualização Tecnológica e Segurança Cibernética:** A aquisição de um Appliance de Firewall de Próxima Geração (NGFW) e de um Console de Gerenciamento modernos proporcionará à ANM uma infraestrutura de segurança atualizada e eficaz, capaz de proteger sua rede contra as mais recentes ameaças cibernéticas.
- **Maior Eficiência e Produtividade:** O uso de equipamentos modernos e um console de gerenciamento avançado permitirá uma gestão mais eficiente e integrada da segurança da rede, aumentando a produtividade da equipe de TI e simplificando as operações de segurança.
- **Redução de Riscos e Vulnerabilidades:** Com a substituição dos firewalls antigos por equipamentos de próxima geração e a implementação de novas medidas de segurança, haverá uma redução significativa nos riscos e vulnerabilidades da rede da ANM, protegendo seus dados e sistemas de possíveis ataques.
- **Capacitação da Equipe:** O treinamento oficial de firewall proporcionará à equipe da ANM o conhecimento necessário para operar e manter os novos equipamentos de segurança de forma eficaz, garantindo o aproveitamento máximo dos recursos disponíveis e a rápida resposta a incidentes de segurança.
- **Conformidade com Regulamentações:** A modernização da infraestrutura de segurança da ANM ajudará a garantir a conformidade com regulamentações e padrões de segurança cibernética, fortalecendo a credibilidade da organização e evitando possíveis penalidades por não conformidade.
- **Flexibilidade e Escalabilidade:** Os novos equipamentos NGFW e o console de gerenciamento oferecerão maior flexibilidade e escalabilidade para acompanhar o crescimento e as demandas futuras da rede da ANM, garantindo que a infraestrutura de segurança possa se adaptar às mudanças no ambiente de TI.
- **Redução de Custos a Longo Prazo:** Embora o investimento inicial possa ser significativo, a substituição dos firewalls antigos e a modernização da infraestrutura de segurança trarão benefícios a longo prazo, incluindo uma redução nos custos de manutenção, menor exposição a ameaças cibernéticas e uma maior eficiência operacional.

#### 3.5. O objeto da contratação está previsto no Plano de Contratações Anual 2025, conforme detalhamento a seguir:

- 3.5.1. ID PCA no PNCP: [29406625000130-0-000002/2025](#)
- 3.5.2. Data de publicação no PNCP: [04/04/2025](#)
- 3.5.3. Id do item no PCA: [238](#)
- 3.5.4. Classe/Grupo: [7050](#)
- 3.5.5. Identificador da Futura Contratação: [323102-161/2025](#)

3.6. O objeto da contratação também está alinhado com a Estratégia de Governo Digital [para o período de 2024 a 2027](#) e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) [2023-2025 da ANM](#), conforme demonstrado abaixo:

#### ALINHAMENTO AOS PLANOS ESTRATÉGICOS

##### ID   Objetivos Estratégicos

**N1 Plano Estratégico ANM 2024-2027 - OE 5 - GARANTIR A EVOLUÇÃO TECNOLÓGICA CONTRIBUINDO PARA GESTÃO EFICIENTE** "Fomentar a modernização e expansão dos recursos de Tecnologia da Informação e Comunicação, aprimorando o desenvolvimento de serviços e soluções alinhadas à eficácia na gestão da Agência Nacional de Mineração (ANM)" IE5.1 Índice de Governança de Tecnologia da Informação (IGOVSISP).

**M1   Objetivo 4 - Plano de Estratégia Nacional de Governo Digital 2024 a 2027 - Privacidade e Segurança - Recomendação 4.1:** "Instituir estrutura de governança e coordenação para implementação de medidas de reforço à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, em articulação com estruturas de mesmo propósito de âmbito regional e nacional, em especial o Programa de Privacidade e Segurança da Informação – PPSI do governo federal."

M2 Objetivo 4 - Plano de Estratégia Nacional de Governo Digital 2024 a 2027 - Privacidade e Segurança - Recomendação 4.2:" Estabelecer plano de ação de reforço à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética que contemple diagnóstico, controles, metodologias e soluções tecnológicas adequadas aos riscos identificados."

ALINHAMENTO AO PDTIC ANM 2023-2025

ID Ação do PDTIC ID Meta do PDTIC associada

A1 PDTIC ANM 2023-2025 ação "A12 - Atualização Periódica do parque tecnológico de equipamentos de TIC"

A2 PDTIC ANM 2023-2025 ação "A20 - Implementar soluções de segurança da informação"

~~3.7. Por tratar de oferta de serviços públicos digitais, o objeto da contratação será integrado à Plataforma Gov.br, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações, de acordo com as especificações deste Termo de Referência.~~

Justificativa: A solução contratada pela Agência Nacional de Mineração (ANM) é **ad personam**, ou seja, atende exclusivamente às necessidades específicas da própria agência, portanto, esta solução não se enquadra na Plataforma Gov.br, conforme estabelecido pelo Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações. As especificações deste Termo de Referência demonstram que a solução é personalizada e não possui aplicabilidade geral para outros órgãos ou entidades governamentais, justificando assim a exclusão da sua integração com a Plataforma Gov.br.

4. Requisitos da contratação

Requisitos de Negócio:

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

4.1.1. 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.

4.1.2. 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.

4.1.3. 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.

4.1.4. 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.

4.1.5. 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.

4.1.6. 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.

4.1.7. 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.

4.1.8. 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.

4.1.9. 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.

4.1.10. 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.



4.1.11. 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.

4.1.12. 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.

4.1.13. 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.

4.1.14. 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.

4.1.15. Custo-efetividade: A solução deve oferecer um bom custo-benefício, equilibrando os custos iniciais de aquisição e implementação com os benefícios de segurança e eficiência operacional a longo prazo.

#### **Requisitos de Capacitação:**

4.2. 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:

4.2.1. A CONTRATADA deverá indicar um técnico habilitado, com profundo conhecimento na solução NGFW ofertada, para ministrar o treinamento técnico especializado.

4.2.2. 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.

4.2.3. 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:**

4.3. 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:**

~~4.4. Devido às características da solução, há necessidade de realização de manutenções (corretivas/preventivas/adaptativa/evolutiva) pela Contratada, visando à manutenção da disponibilidade da solução;~~

4.4. Devido às características da solução se faz necessário, no âmbito do item 1, a manutenção observando os seguintes requisitos:

4.4.1. A CONTRATANTE notificará a CONTRATADA através de comunicação oficial na ocorrência de defeitos nos equipamentos fornecidos, durante o período de garantia estendida.

4.4.2. 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.

4.4.3. 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.

4.4.4. Alegado defeito por mau uso, ficam os prazos da comunicação oficial suspensos até avaliação da CONTRATANTE do Laudo Técnico emitido pela CONTRATADA.

4.4.5. 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.

4.4.6. 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.

4.4.7. 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:

4.5. 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:

4.5.1. 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.

4.6. 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.

4.6.1. 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.

4.6.2. 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

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

4.7.1. 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.

4.7.2. 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.

4.7.3. 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.

4.7.4. 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 antispam e antivírus.

4.7.5. 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.

4.7.6. 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:

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

4.8.1. 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.

4.8.2. 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.

4.8.3. 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.

4.8.4. 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:**

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

4.10. 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:**

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

4.11.1. 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.

4.11.2. 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.

4.11.3. 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.

4.11.4. 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.

4.11.5. 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.

4.11.6. 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.

4.11.7. 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.

4.11.8. 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:

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

4.12.1. 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.

4.12.2. 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.

4.12.3. A instalação deverá ocorrer na Sede da CONTRATANTE.

4.12.4. 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.

4.12.5. 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.

4.12.6. 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.

4.12.7. 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.

4.12.8. 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).

4.13. Deverão ser realizadas as seguintes atividades mínimas:

4.13.1. Instalação física no Datacenter da CONTRATANTE.

4.13.2. Configuração Inicial do sistema, incluindo configuração de acesso de gerenciamento ao sistema (usuários e senhas), configuração inicial dos equipamentos.

4.13.3. Configuração de rede/VLAN.

4.13.4. Realização de testes de funcionamento dos equipamentos.

4.13.5. Realização de testes de funcionamento de acesso.

4.13.6. Atualização do firmware/sistema operacional dos sistemas e equipamentos.

4.13.7. Demais atividades necessárias para o perfeito funcionamento dos sistemas.

4.13.8. 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:

4.14. 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 à assistência técnica quando demandada:

4.14.1. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

4.14.2. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

- 4.14.3. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.
- 4.14.4. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.
- 4.14.5. Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 30 (trinta) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.
- 4.14.6. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.
- 4.14.7. Na hipótese do subitem acima, o Contratado deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.
- 4.14.8. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.
- 4.14.9. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.
- 4.14.10. A garantia legal ou contratual do objeto tem prazo de vigência própria e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.
- 4.14.11. Deverão ser observadas as demais exigências de assistência técnica e de manutenção exigidas no Termo de Referência (TR) e seus anexos.

4.15. 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**

4.16. 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**

4.17. Os serviços deverão ser prestados por técnicos devidamente capacitados.

#### **Requisitos de Metodologia de Trabalho**

Relativo aos serviços,

4.18. 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.

4.19. 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.

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

Relativo aos bens,

4.21. O fornecimento dos equipamentos está condicionado ao recebimento pelo Contratado de Ordem de fornecimento de Bens (OFB) emitida pela Contratante.

4.22. A OFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

4.23. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e 8 horas por dia e 7 dias por semana por via telefônica.

4.24. O andamento do fornecimento dos equipamentos deve ser acompanhado pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

## Requisitos de Segurança da Informação e Privacidade

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

- 4.25.1. Normas de Segurança da Informação e Privacidade descritas na POSIC da ANM;
- 4.25.2. Lei Nº 13.708, de 14 de agosto de 2018 Lei Geral de Proteção de Dados Pessoais;
- 4.25.3. Decreto Nº 9.637, de 26 de dezembro de 2018 Institui a Política Nacional de Segurança da Informação;
- 4.25.4. 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;
- 4.25.5. 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;
- 4.25.6. 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;
- 4.25.7. 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;
- 4.25.8. 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;
- 4.25.9. 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;
- 4.25.10. ABNT NBR ISO 22301:2013 Sistemas de gestão de continuidade de negócios;
- 4.25.11. ABNT NBR ISO 22313:2015 Sistemas de gestão de continuidade de negócios;
- 4.25.12. ABNT NBR ISO 27031:2015 Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação;
- 4.25.13. ABNT NBR 11515:2007 Guia de práticas para segurança física relativas ao armazenamento de dados;
- 4.25.14. ABNT NBR ISO/IEC 27002:2013 Código de prática para controles de segurança da informação;
- 4.25.15. ABNT NBR ISO/IEC 27014:2013 Governança de segurança da informação;
- 4.25.16. A CONTRATADA não pode obter, capturar, copiar ou transferir qualquer tipo informação de propriedade da CONTRATANTE, sem autorização.
- 4.25.17. 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.
- 4.25.18. 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 devese abster de divulgar ou repassar quaisquer dados ou informações, salvo se expressamente autorizado pela CONTRATANTE.
- 4.25.19. Outras medidas indicadas durante a vigência do contrato pela CONTRATANTE.

## Vistoria

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

## Outros Requisitos Aplicáveis

4.27. Não se aplica.

## Sustentabilidade:

4.28. 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):**

4.29. Não se aplica.

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

4.30. Não se aplica.

**Da exigência de carta de solidariedade:**

4.31. Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato ou declaração de revenda autorizada, que assegure a plena execução do contrato. Este documento deverá garantir, de maneira clara, que, na hipótese de eventual incapacidade técnica ou operacional do revendedor ou distribuidor, o fabricante assumirá o compromisso de prestar o suporte necessário ao cumprimento das obrigações contratuais, resguardando a continuidade do fornecimento e a qualidade dos "appliances" adquiridos (item 1 do objeto) e do serviço de "console de gerenciamento" (item 2 do objeto).

**Justificativa:** A presente exigência nesse processo licitatório para aquisição de solução de firewall e serviços correlatos, com respaldo na Lei nº 14.133/2021, em seu art. 41, inciso IV, é feita em estrita observância aos princípios da eficiência, segurança e continuidade dos serviços públicos se justifica sobretudo por: (a) 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. (b) 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. (c) 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. (d) Mitigação de Riscos Operacionais: A carta de solidariedade ou declaração de revenda autorizada, 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. (e) 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**

4.32. Não é admitida a subcontratação do objeto contratual.

**Da verificação de amostra do objeto**

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

**Garantia da Contratação**

4.34. 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 por cento) do valor contratual, conforme regras previstas no contrato.

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

4.36. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.37. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

**Informações relevantes para o [dimensionamento E/OU apresentação] da proposta**

4.38. Não se aplica.

## 5. Papéis e responsabilidades

### 5.1. São obrigações da CONTRATANTE:

- 5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- 5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;
- 5.1.3. receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- 5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- 5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- 5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- 5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável;
- 5.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

### 5.2. São obrigações do CONTRATADO:

- 5.2.1. indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;
- 5.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- 5.2.3. reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato pela Contratante;
- 5.2.4. propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;
- 5.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- 5.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- 5.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;
- 5.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;
- 5.2.9. fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso;

### 5.3. São obrigações do órgão gerenciador do registro de preços:

- 5.3.1. efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;
- 5.3.2. conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;
- 5.3.3. definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:
  - 5.3.3.1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e
  - 5.3.3.2. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;
- 5.3.4. definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:



5.3.4.1. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

5.3.4.2. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo contratado; e

5.3.4.3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 do art. 17 da Instrução Normativa SGS/ME nº 94, de 2022, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

## 6. Modelo de execução do contrato

### DOS BENS

#### Rotinas de Execução

##### Do Encaminhamento Formal de Demandas:

6.1. O gestor do contrato emitirá a Ordem de fornecimento de bens (OFB) para a entrega dos bens desejados.

6.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na OFB.

6.3. O recebimento provisório e definitivo dos bens é disciplinado em tópico próprio deste TR.

##### Forma de execução e acompanhamento do contrato:

#### Condições de Entrega

6.4. O prazo máximo de entrega dos bens é de 15 (quinze) dias, contados da emissão da Ordem de fornecimento de bens (OFB), em remessa única, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

6.5. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 5 (cinco) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

6.6. Os bens deverão ser entregues no seguinte endereço: SERPRO Sede - SGAN Quadra 601 Módulo "V" Brasília - DF CEP: 70836-900.

6.7. 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.

##### Formas de transferência de conhecimento:

6.8. A transferência do conhecimento deverá ser realizada observando-se o que segue:

- 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.
- Deverá ser providenciada a documentação completa do processo de implantação, incluindo todas as configurações realizadas e decisões tomadas, em formato legível e tecnicamente fundamentado.
- 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.
- 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.
- Deverá ser observada as demais condições específica definidas neste Edital.

#### **Procedimentos de transição e finalização do contrato**

6.9. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

#### **Quantidade mínima de bens ou serviços para comparação e controle**

6.10. Cada OFB conterá a quantidade a ser fornecida, incluindo a sua localização e o prazo, conforme definições deste TR.

#### **Mecanismos formais de comunicação:**

6.11. São definidos como mecanismos formais de Comunicação, entre a Contratante e o Contratado, os seguintes:

- Ordem de Fornecimento de Bens;
- Ata de Reunião;
- Ofício;
- Sistema de abertura de chamados;
- E-mails e Cartas;
- [Transcrições de reuniões;](#)
- [Gravações de reuniões do teams;](#)
- [Mensagens de aplicativos de mensagens.](#)

#### **Formas de Pagamento:**

6.12. Os critérios de medição e pagamento serão tratados [no item 7 e seguintes deste Termo de Referência.](#)

#### **Manutenção de Sigilo e Normas de Segurança:**

6.13. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução do contrato, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.14. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se anexo a este Edital.

### **DOS SERVIÇOS**

Justificativa: Foi necessária a inclusão dos tópicos relativos a serviços neste Termo de Referência, considerando que o modelo da AGU apresenta versões separadas para contratações exclusivamente de bens ou exclusivamente de serviços. No entanto, nas aquisições de bens de TIC, é comum e essencial a contratação de serviços acessórios especializados, como instalação, configuração e operação assistida. Esses serviços demandam condições específicas de gestão e acompanhamento, como definição de SLA, designação de preposto, emissão de ordens de serviço, entre outros, os quais estão estruturados apenas no modelo de serviços da AGU. Por esse motivo, optou-se por incorporar integralmente os trechos pertinentes ao modelo de serviços ao presente TR, garantindo maior robustez e adequação à natureza híbrida do objeto.

6.15. O modelo de execução dos serviços se encontra detalhado no "ANEXO C – Informações Complementares sobre o Modelo de Execução dos Contratos".

## **7. Modelo de gestão do contrato**

### **MODELO DE GESTÃO DO CONTRATO RELATIVO AOS BENS (ITEM 1)**

Justificativa: Foi necessária a inclusão dos tópicos relativos a serviços neste Termo de Referência, considerando que o modelo da AGU apresenta versões separadas para contratações exclusivamente de bens ou exclusivamente de serviços. No entanto, nas aquisições de bens de TIC, é comum e essencial a contratação de serviços acessórios especializados, como instalação, configuração e operação assistida. Esses serviços demandam condições específicas de gestão e acompanhamento, como definição de SLA, designação de

preposto, emissão de ordens de serviço, entre outros, os quais estão estruturados apenas no modelo de Justificativa: Foi necessário incluir tópicos relativos a serviços neste Termo de Referência, pois o modelo da AGU apresenta versões separadas para contratações de bens e serviços. Nas aquisições de bens de TIC, é comum e essencial contratar serviços acessórios especializados, como instalação, configuração e operação assistida. Esses serviços exigem condições específicas de gestão e acompanhamento, como definição de SLA, designação de preposto e emissão de ordens de serviço, que estão estruturados apenas no modelo de serviços da AGU. Por isso, optou-se por incorporar integralmente os trechos pertinentes ao modelo de serviços ao presente TR, garantindo maior robustez e adequação à natureza híbrida do objeto. Além disso, há divergências textuais entre o modelo de Termo de Referência (TR) do Compras.gov.br e o Modelo de Termo de Referência Compras TIC - Lei 14.133 (maio/23) da AGU. O TR do Compras.gov.br, cuja versão vigente é de julho de 2023, é de preenchimento obrigatório e não possui o item "8. Critérios de Medição e de Pagamento", presente na versão de maio/2023, estando essas informações no item "7. Modelo de gestão do contrato". Não é possível renomear o item "8. Do reajuste" para "8. Critérios de Medição e de Pagamento" devido às restrições do sistema. O preenchimento do TR no Compras.gov.br é requisito técnico para a tramitação do processo. Portanto, optou-se por manter a estrutura do modelo do TR no Compras.gov.br, com os Critérios de Medição e de Pagamento no item "7. Modelo de gestão do contrato".

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

### **Reunião Inicial**

7.5. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução do contrato.

7.6. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até **05 (cinco)** dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.7. A pauta desta reunião observará, pelo menos:

7.7.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.7.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

7.7.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.7.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.7.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

### **Fiscalização**

7.8. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput) , nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

### **Fiscalização Técnica**

7.9. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

7.9.1. O fiscal técnico do contrato anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

7.9.2. Identificada qualquer inexistência ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

7.9.3. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

7.9.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

7.9.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

### **Fiscalização Administrativa**

7.10. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

7.10.1. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

7.11. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

#### **7.11.1 Conformidade com as normas de gestão estabelecidas pela contratante.**

### **Gestor do Contrato**

7.12. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

7.13. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

7.14. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

7.15. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

7.16. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

7.17. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual. (Decreto nº 11.246, de 2022, art. 22, VII).

7.18. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

### **Critérios de Aceitação**

7.19. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

7.20. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não reconicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).

7.21. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos

não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

7.22. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

7.23. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

7.24. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

7.25. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

7.26. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

7.27. A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.

7.28. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJE-TO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

Procedimentos de Teste e Inspeção

7.29. Serão adotados como procedimento de teste e inspeção, para fins de elaboração dos Termo de Recebimento Provisório e Definitivo:

7.29.1. A checagem do atendimento às especificações do edital será realizada por meio de testes de conformidade técnica conduzidos pela equipe da CONTRATANTE, imediatamente após a entrega provisória dos equipamentos. Serão verificados aspectos como as características físicas (número e tipo de interfaces), desempenho declarado no datasheet oficial do fabricante, presença e validade das licenças, compatibilidade com os requisitos técnicos descritos no Termo de Referência e a integridade física do equipamento. Apenas após a validação de todos os requisitos será emitido o termo de recebimento definitivo.

Níveis Mínimos de Serviço Exigidos

7.30. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO		
Tópico	Descrição	
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens.	
Meta a cumprir	IAE <= 0	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento de Bens dentro do prazo previsto.
Instrumento de medição	OFB, Termo de Recebimento Provisório (TRP)	
	A avaliação será feita conforme linha de base do cronograma registrada na OFB.	

Forma de acompanhamento	Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB.
Periodicidade	Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.
Mecanismo de Cálculo (métrica)	<p>IAE = TEX – TEST</p> <p>Onde:</p> <p>IAE – Indicador de Atraso de Entrega da OFB;</p> <p>TEX – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB.</p> <p>A data de início será aquela constante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB.</p> <p>A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quanto o Contratado entrega os produtos da OFB e haja aceitação por parte do fiscal técnico.</p> <p>TEST – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.</p>
Observações	<p>Obs1: Serão utilizados dias corridos na medição.</p> <p>Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.</p>
Início de Vigência	A partir da emissão da OFB.
Faixas de ajuste no pagamento e Sanções	<p>Para valores do indicador IAE:</p> <p>Menor ou igual a 0 – Pagamento integral da OFB;</p> <p>De 1 a 60 - aplicar-se-á glosa de 0,1666% por dia de atraso sobre o valor da OFB ou fração em atraso.</p> <p>Acima de 60 - aplicar-se-á glosa de 10% bem como multa de 2% sobre o valor OFB ou fração em atraso.</p>

**Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento**

7.31. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

IAP – ÍNDICE DE ATENDIMENTO NO PRAZO	
Tópico	Descrição
Finalidade	Medir o tempo de atraso na prestação dos serviços constantes na Ordem de Serviço.
Meta a cumprir	IAP igual ou superior a 90 (noventa) %.



<b>Instrumento de medição</b>	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
<b>F o r m a de acompanhamento</b>	É apurado pelos fiscais do contrato avaliando a quantidade atendida dentro do prazo em relação à quantidade total atendida no período de referência.
<b>Periodicidade</b>	Mensal
<b>Mecanismo de Cálculo (métrica)</b>	$IAP = 100 * (\Sigma Q_{tap} / \Sigma Q_{tr})$ <p>Onde:</p> <p>IAP = Indicador de atendimento aos prazos do serviço;</p> <p><math>\Sigma Q_{tap}</math> = Somatório do quantitativo atendido no prazo máximo estabelecido no TR com previsão de encerramento para o período de referência;</p> <p><math>\Sigma Q_{tr}</math> = Somatório do quantitativo total registrado com previsão de encerramento para o período de referência.</p>
<b>Observações</b>	<p>Obs1: Serão utilizados dias corridos na medição.</p> <p>Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.</p>
<b>Início de Vigência</b>	A partir da emissão da OS.
<b>Faixas de ajuste no pagamento e Sanções</b>	<p>IAP <math>\geq</math> 90%: sem descontos sobre o valor da fatura mensal.</p> <p>IAP <math>\geq</math> 80% e <math>&lt;</math> 90%: 10% de desconto sobre o valor da fatura mensal.</p> <p>IAP <math>\geq</math> 70% e <math>&lt;</math> 80%: 20% de desconto sobre o valor da fatura mensal.</p> <p>IAP <math>&lt;</math> 70%: 30% de desconto sobre o valor da fatura mensal.</p>

7.32. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o Contratado:

7.32.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

7.32.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

### Critérios de medição e de pagamento

#### Recebimento do objeto

7.33. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

7.34. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de **05 (cinco)** dias, a contar da notificação do Contratado, às suas custas, sem prejuízo da aplicação das penalidades.

7.35. O recebimento definitivo ocorrerá no prazo de **05 (cinco)** dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

7.36. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até **05 (cinco)** dias úteis.

7.37. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

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

7.39. O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

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

## **LIQUIDAÇÃO, PRAZO DE PAGAMENTO, FORMA DE PAGAMENTO E CESSÃO DE CRÉDITO (ITENS 1, 2, 3, 4 e 5)**

### **Liquidação**

7.41. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

7.41.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

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

- 7.42.1. o prazo de validade;
- 7.42.2. a data da emissão;
- 7.42.3. os dados do contrato e do órgão Contratante;
- 7.42.4. o período respectivo de execução do contrato;
- 7.42.5. o valor a pagar; e
- 7.42.6. eventual destaque do valor de retenções tributárias cabíveis.

7.43. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante;

7.44. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

7.45. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

7.46. Constatando-se, junto ao SICAF, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

7.47. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.48. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

7.49. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o Contratado não regularize sua situação junto ao SICAF.

#### **Prazo de pagamento**

7.50. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

7.51. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice [ICTI](#) de correção monetária.

#### **Forma de pagamento**

7.52. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

7.53. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.54. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.55. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

7.56. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

#### **Cessão de crédito**

7.57. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.

7.58. As cessões de crédito não fiduciárias dependerão de prévia aprovação do Contratante.

7.59. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

7.60. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 7.429, de 1992, tudo nos termos do Parecer JL-01, de 18 de maio de 2020.

7.61. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

7.62. A cessão de crédito não afetará a execução do objeto Contratado, que continuará sob a integral responsabilidade do Contratado.

#### **MODELO DE GESTÃO DO CONTRATO RELATIVO AOS SERVIÇOS (ITENS 2, 3, 4 e 5)**

Justificativa: Foi necessário incluir tópicos relativos a serviços neste Termo de Referência, pois o modelo da AGU apresenta versões separadas para contratações de bens e serviços. Nas aquisições de bens de TIC, é comum e essencial contratar serviços acessórios especializados, como instalação, configuração e operação assistida. Esses serviços exigem condições específicas de gestão e acompanhamento, como definição de SLA, designação de preposto e emissão de ordens de serviço, que estão estruturados apenas no modelo de serviços da AGU. Por isso, optou-se por incorporar integralmente os trechos pertinentes ao modelo de serviços ao presente TR, garantindo maior robustez e adequação à natureza híbrida do objeto. Além disso, há divergências textuais entre o modelo de Termo de Referência (TR) do Compras.gov.br e o Modelo de Termo de Referência Compras TIC - Lei 14.133 (maio/23) da AGU. O TR do Compras.gov.br, cuja versão vigente é de julho de 2023, é de preenchimento obrigatório e não possui o item "8. Critérios de Medição e de Pagamento", presente na versão de maio/2023, estando essas informações no item "7. Modelo de gestão do contrato". Não é possível renomear o item "8. Do reajuste" para "8. Critérios de Medição e de Pagamento" devido às restrições do sistema. O preenchimento do TR no Compras.gov.br é requisito técnico para a tramitação do processo. Portanto, optou-se por manter a estrutura do modelo do TR no Compras.gov.br, com os Critérios de Medição e de Pagamento no item "7. Modelo de gestão do contrato".

7.63. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.64. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.65. As comunicações entre o órgão ou entidade e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.66. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

### **Preposto**

7.67. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

7.68. A Contratada deverá manter preposto da empresa no local da execução do objeto durante o período [demandado pela Contratante](#).

7.69. Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade

### **Reunião Inicial**

7.70. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

7.71. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até [5 \(cinco\)](#) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.71.1. A pauta desta reunião observará, pelo menos:

7.71.1.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.71.1.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

7.71.1.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.71.1.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.71.1.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

### **Fiscalização**

7.72. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput) , nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

#### **Fiscalização Técnica**

7.73. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

7.73.1. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

7.73.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

7.73.3. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

7.73.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

7.73.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

### **Fiscalização Administrativa**

7.74. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

7.74.1. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

7.75. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

7.75.1. [Conformidade com as normas de gestão estabelecidas pela contratante.](#)

### **Gestor do Contrato**

7.76. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

7.77. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

7.78. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

7.79. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

7.80. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

7.81. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

7.82. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

### **Critérios de medição e pagamento**

7.83. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), conforme previsto no [Anexo B deste Termo de Referência](#).

7.84. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

7.84.1. não produzir os resultados acordados;

7.84.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

7.84.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

7.85. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

7.86. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

**7.86.1. Níveis de severidade do chamado conforme previsto no Anexo B deste Termo de Referência.**

## **Do recebimento**

7.87. Os serviços serão recebidos provisoriamente, no prazo de **5 (cinco)** dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a, da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

7.87.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

7.88. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).

7.89. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)

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

7.91. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

7.92. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

7.93. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.94. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

7.95. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.96. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

7.97. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

7.98. Os serviços serão recebidos definitivamente no prazo de **5 (cinco)** dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

7.98.1 Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

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

7.98.3 Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas;

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

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



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

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

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

**Procedimento de Teste de Inspeção**

7.102. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

a) Conforme definidos no Anexo B e Anexo C deste Termo de Referência.

**Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento**

7.103. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela contratante, conforme a tabela abaixo:

Id Ocorrência		Glosa / Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução do contrato dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 16 horas úteis.	Multa de 0,5 % sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 5 (cinco) dias úteis.
		Após o limite de 5 (cinco) dias úteis, aplicar-se-á multa de 0,75 % do valor total do Contrato.
2	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS)	Glosa de 0,5 % sobre o valor da OS para valores do indicador IAE de 0,11 a 0,20.
		Glosa de 0,5 % sobre o valor da OS para valores do indicador IAE de 0,21 a 0,30.
		Glosa de 0,5 % sobre o valor da OS para valores do indicador IAE de 0,31 a 0,50.
		Glosa de 0,5 % sobre o valor da OS para valores do indicador IAE de 0,51 a 1,00.
		Multa de 0,5 % sobre o valor do Contrato e Glosa de 0,5 % sobre o valor da OS, para valores do indicador IAE maiores que 1,00.
3	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 0,5 % do valor total do Contrato.

7.104. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que p contratado:

7.104.1 não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

7.104.2 deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

## 8. Do reajuste

### 8.1. Será adotado como índice de reajuste do Contrato o Índice de Custos de Tecnologia da Informação – ICTI.

Justificativa: Existe divergência textual entre o modelo de Termo de Referência (TR) disponibilizado pelo Compras.gov.br, relativo ao item 8, na forma de artefato digital obrigatório (art. 9, § 7º, Instrução Normativa SGD/ME nº 94, de 2022), e o Modelo de Termo de Referência Compras TIC - Lei 14.133 (maio/23) constante na página da AGU, no Portal de Compras do Governo Federal e nos Templates da SGD. Destaca-se que o TR no Compras.gov.br, cuja versão vigente é de julho de 2023, é de preenchimento obrigatório e não permite a exclusão do referido item, e tampouco é devida a inserção da expressão "Não se Aplica". O preenchimento do TR no Compras.gov.br é requisito técnico para a tramitação do processo. Portanto, optou-se por manter o item conforme a estrutura padrão do sistema. Ressalta-se, contudo, que os aspectos relacionados ao Reajuste já estão adequadamente abordados e detalhados no artefato Contrato, de modo que não há prejuízo à clareza, à legalidade ou à integridade das informações exigidas para a contratação. Diante disto, justifica-se a manutenção do item "8. Do Reajuste" conforme previsto no sistema Compras.gov.br.

## 9. Critérios de seleção do fornecedor

### Forma de seleção e critério de julgamento da proposta

9.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo **menor preço**.

#### 9.1.1. A contratação da solução de TIC será realizada por meio do Sistema de Registro de Preços.

### Da Aplicação da Margem de Preferência

9.2. Não será aplicada margem de preferência na presente contratação.

### Exigências de habilitação

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

#### Habilitação jurídica,

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

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

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

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

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

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

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

9.11. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

#### **Habilitação fiscal, social e trabalhista**

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

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

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

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

9.17. Prova de inscrição no cadastro de contribuintes [Estadual/Distrital](#) e [Municipal/Distrital](#) relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.18. Prova de regularidade com a Fazenda [Estadual/Distrital](#) e [Municipal/Distrital](#) do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

9.19. Caso o fornecedor seja considerado isento dos tributos [Estadual/Distrital](#) e [Municipal/Distrital](#) relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

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

#### **Qualificação Econômico-Financeira**

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

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

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

9.23.1 Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

9.23.2 As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

9.23.3 Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

9.23.4 Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

9.24. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação [capital mínimo de 10% do valor total estimado da contratação](#).

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

9.26. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

#### **Qualificação Técnica**

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

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

9.27.1.1. Atestado de fornecimento de NGFW: Comprovar a entrega de appliance de firewall de próxima geração (NGFW) com características técnicas similares ao objeto, incluindo modelos compatíveis em porte e funcionalidades.

9.27.1.2. Atestado de prestação de serviços de instalação e configuração de NGFW: Comprovar que a empresa instalou e configurou soluções NGFW, preferencialmente de porte e complexidade similares, inclusive integração com infraestrutura de rede e segurança.

9.27.1.3. Atestado de prestação de serviços de operação assistida ou suporte técnico especializado: Demonstrar experiência em prover serviços de apoio técnico contínuo, como operação assistida, troubleshooting ou suporte de segundo/terceiro nível em ambiente de segurança da informação.

9.27.1.4. Obs.: A licitante deverá apresentar uma planilha que associe os atestados por ela apresentados às respectivas exigências acima.

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

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

9.27.4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da Contratante e local em que foi executado o objeto Contratado, dentre outros documentos.

~~9.28. Na fase de habilitação técnica, a licitante deverá, caso seja fornecedor ou revendedor ou distribuidor, apresentar uma carta de solidariedade emitida pelo fabricante, que assegure a plena execução do contrato. Esse documento deverá garantir que, mesmo na ausência de capacidade técnica ou operacional do revendedor ou distribuidor, o fabricante compromete-se a dar suporte à execução contratual, resguardando a continuidade do fornecimento e a qualidade dos serviços ou bens contratados.~~

~~Justificativa: 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: (a) 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. (b) 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. (c) 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. (d) 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. (e) 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.~~

~~9.29. Não será permitida a participação de consórcios e cooperativas na presente licitação.~~

~~9.29. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:~~

~~9.29.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;~~

~~9.29.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;~~

~~9.29.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;~~

~~9.29.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;~~

~~9.29.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato, e~~

9.29.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa. a) ata de fundação, b) estatuto social com a ata da assembleia que o aprovou, c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia, d) editais de convocação das três últimas assembleias gerais extraordinárias, e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais, e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

9.29.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

Justificativa: Considerando a natureza técnica e operacional do objeto licitado, especialmente no que se refere à complexidade da execução dos serviços envolvidos e à necessidade de gerenciamento centralizado, contínuo e com alto nível de especialização, a participação de cooperativas e consórcios não se mostra adequada ao modelo de contratação adotado. A gestão dos serviços exigidos pressupõe vínculo direto com a contratada, controle efetivo da execução, responsabilização integral e atendimento a requisitos técnicos, operacionais e legais específicos, o que pode ser inviabilizado pela estrutura descentralizada e de cogestão própria de cooperativas e pela composição compartilhada e, muitas vezes, temporária dos consórcios. Adicionalmente, o modelo de gestão previsto para esta contratação exige clareza na cadeia de responsabilidade, rastreabilidade das entregas e aderência a níveis de serviço previamente pactuados, o que reforça a necessidade de contratação de empresa única, especializada, com capacidade técnica e operacional consolidada. Dessa forma, por razões de governança, controle e efetividade contratual, fica vedada a participação de cooperativas e consórcios nesta licitação.

## 10. Estimativas do valor da contratação

Valor (R\$): 2.673.383,88

10.1. O custo estimado total da contratação 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), conforme custos unitários apostos na tabela abaixo:

Grupo	Id	Descrição	Quant.	Unid.	CATSER CATMAT	Valor Unit.	Valor Total
1	1	Appliance de Firewall de próxima geração (NGFW)	2	Unid.	CATMAT 609340	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	Unid.	CATSER 27502	R\$ 180.884,09	R\$ 180.884,09
	3	Serviços de Instalação e Configuração de Firewall de Próxima Geração	1	Unid.	CATSER 27111	R\$ 146.577,73	R\$ 146.577,73
	4	Treinamento técnico especializado na solução de NGFW (uma turma)	1	Unid.	CATSER 16837	R\$ 41.607,93	R\$ 41.607,93
	5	Operação assistida especializada prestada pelo fornecedor (HST)	500	HST	CATSER 27510	R\$ 372,62	R\$ 186.308,69
Total							R\$ 2.673.383,88

10.2. 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).

10.3. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre Contratante e Contratado, conforme especificado na matriz de risco constante do Contrato.

10.4. Em caso de licitação para Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

- 10.4.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;
- 10.4.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;
- 10.4.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou
- 10.4.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

10.5 Para o item 5, a cada ciclo de 12 meses de vigência contratual, os quantitativos de HST originalmente pactuados serão integralmente renovados, independentemente do consumo efetivo de HST registrado no período anterior:

- 10.5.1 Durante a vigência contratual, os totais de HST de operação assistida não utilizados em cada período de 12 (doze) meses, contados a partir da data de assinatura do contrato ou sua renovação, expirarão automaticamente ao final de cada ciclo anual.
- 10.5.2. A cada novo ciclo de 12 (doze) meses, os quantitativos de HST serão integralmente renovados, sendo vedada a acumulação de horas não utilizadas de um ciclo para o outro

## 11. Adequação orçamentária

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

11.2. A contratação será atendida pela seguinte dotação:

- Gestão/Unidade: 32396/323102;
- Fonte de Recursos: 1053000012;
- Programa de Trabalho: PTRES: 235023 - GESTAO DOS RECURSOS DE TECNOLOGIA DA INFORMACAO;
- Elemento de Despesa:
  - Item 1: CATMAT: 609340 - ND 449052.37 - Equipamentos de tic - ativos de rede
  - Item 2: CATSER: 27502 - ND 339040.06 - Locação de Softwares
  - Item 3: CATSER: 27111 - ND 339040.22 - Instalação de Equipamentos de TIC
  - Item 4: CATSER: 16837 - ND 339040.20 - Treinamento/Capacitação em TIC
  - Item 5: CATSER: 27510 - ND 339040.21 - Serviços Técnicos Profissionais de TI
- Plano Interno: Plano Orçamentário: 21F6 - Modernização e Gestão dos Recursos de Tecnologia da Informação e Comunicação;

11.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

### Cronograma Físico Financeiro

Evento	Prazo estimado	Valor
Evento 1	entrega do 2 appliances no SERPRO/DF, 5 (cinco) dias após a emissão da OFB.	Não há
Evento 2	Execução do item 3 (instalação e configuração dos NGFW). concomitante às atividades do Evento 1.	Não há



Evento 3	Recebimento provisórios, recebimento definitivo, ateste e pagamento dos itens 1 e 3, pagamento em até 10 (dez) após o ateste.	R\$ 2.264.583,17
Evento 4	Execução do treinamento (item 4), 5 (cinco) dias após a emissão da Ordem de serviço, pagamento em até 10 (dez) após o ateste.	R\$ 41.607,93
Evento 5	Ativação do console de gerenciamento do NGFW, concomitante às atividades do Evento 1, pagamento em até 10 (dez) após o ateste.	R\$ 180.884,09
Evento 6	Execução do serviços de operação assistida (sob situação de contingência e sob demanda), sem prazo para iniciar.	Não há

## 12. 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**

Requisitante



Assinou eletronicamente em 01/09/2025 às 08:15:32.

**MARCIO JOSE ANTUNES GOMES**

Integrante Técnico



Assinou eletronicamente em 01/09/2025 às 08:51:05.

**NEWTON TAKESHI OKUNO**

Integrante Administrativo



Assinou eletronicamente em 01/09/2025 às 13:15:33.

**FABIO FERNANDO BORGES**

Autoridade competente

## Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - ANEXOS A B e C - TR NGFW v.2.pdf (1.88 MB)

## ANEXO A – DESCRIÇÃO TÉCNICA DA SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

### PADRONIZAÇÃO E GARANTIA DE COMPATIBILIDADE

- O item 1 tem como finalidade substituir o appliance atualmente instalado, mantendo inalterada a topologia e a infraestrutura de conectividade já existente (incluindo switches, cabeamento e racks), de modo a assegurar a continuidade operacional sem a necessidade de reconfigurações na rede e substituição de mais equipamentos, reduzindo o custo para a Administração.
- Para assegurar a padronização e garantir a plena compatibilidade técnica, funcional e operacional, inclusive em futuras atualizações e upgrades, os itens 1 e 2 deverão, obrigatoriamente, ser fornecidos pelo mesmo fabricante. Essa exigência visa evitar problemas de interoperabilidade, maximizar o desempenho do sistema e garantir o suporte adequado durante o ciclo de vida da solução.
- Para garantir a execução adequada do contrato, especialmente nos casos em que o licitante não seja o fabricante direto dos bens ou equipamentos a serem fornecidos, mas atue como revendedor ou distribuidor, é necessário apresentar uma Carta de Solidariedade emitida pelo fabricante. Este documento deve assegurar o compromisso do fabricante com a qualidade, a disponibilidade dos produtos e o suporte necessário durante a vigência contratual, estabelecendo responsabilidade solidária entre o fabricante e o licitante quanto ao cumprimento integral das obrigações contratuais.

#### Item 1 – Appliance de Firewall de próxima geração (NGFW),

##### CARACTERÍSTICAS GERAIS MÍNIMAS PARA FIREWALLS DE PRÓXIMA GERAÇÃO

##### Hardware e Arquitetura,

- Appliance dedicado com funcionalidades de NGFW e NGIPS, fornecido com hardware e software integrados.
- Montagem em rack 19 polegadas, com kits de trilhos e acessórios incluídos.
- Fonte de alimentação redundante e hot-swappable.
- Disco SSD com capacidade mínima de 240 GB (para armazenamento de logs e operações críticas).
- Interfaces mínimas suportadas:
  - 1 portas USB 2.0 (ou superior)
  - 1 porta de gerenciamento RJ45 Gigabit Ethernet (GE)
  - 8 portas RJ45 Gigabit Ethernet (GE)
  - 8 slots SFP Gigabit Ethernet (GE)
  - 4 slots SFP+/SFP 10G/1G (10GE/GE)
  - 4 slots SFP28/SFP+ 25G/10G
- Todas as portas físicas do appliance de firewall deverão ser entregues devidamente populadas com os respectivos pares de transceptores ópticos (GBICs) e respectivos cabos compatíveis com o modelo do equipamento e homologados pelo respectivo fabricante considerando sempre as maiores velocidades das portas. Essa exigência visa garantir plena funcionalidade, desempenho ideal e a conformidade técnica do equipamento, eliminando possíveis problemas de compatibilidade e assegurando que todos os recursos estejam disponíveis para a operação desde a sua instalação e possibilitando o uso imediato das interfaces especificadas.

#### Desempenho,

Considerando que o equipamento especificado no Item 1 tem como objetivo substituir o NGFW atualmente em uso, é fundamental que a nova solução apresente valores de desempenho iguais ou superiores aos do equipamento em operação, garantindo a manutenção da capacidade de processamento, segurança e eficiência da infraestrutura de rede da Agência.

- Throughput **mínimo**:
  - 13 Gbps de throughput para IPS
  - 10.5 Gbps de throughput para inspeção SSL
  - 12 Gbps de throughput para controle de aplicações
  - 4 Gbps de Throughput SSL-VPN
  - 7 Gbps de throughput para NGFW
  - 5 Gbps de throughput para proteção contra ameaças
- Suporte para no mínimo: **12 milhões de sessões TCP** em um cenário padrão (sem picos) e **300 mil novas conexões TCP** a cada segundo também para cenário padrão.

#### Funcionalidades NGFW,

- Reconhecimento de aplicações, prevenção de ameaças (IPS/IDS), controle de permissões e filtragem de URL.
- Suporte para virtualização de no **mínimo**:
  - 10 sistemas virtuais lógicos.
  - 1.500 clientes VPN SSL simultâneos.
  - 500 túneis VPN IPsec simultâneos.

#### Gerenciamento e Monitoramento,

- Console abrangente para gestão centralizada e monitoramento.
- Interface de linha de comando (CLI), interface gráfica (GUI) e acesso remoto via porta serial.
- Suporte para backup/restauração local ou remoto (FTP/e-mail).

#### Atualizações e Suporte,

A garantia para os appliances de firewall deverão ser de no mínimo 60 (sessenta) meses, contados a partir da aceitação definitiva dos equipamentos. Durante todo o período de garantia, a contratada deverá assegurar:

- Manutenção e suporte completo ao hardware: Todos os componentes do hardware, incluindo placa-mãe, processador, memória, disco rígido, fonte de alimentação, e quaisquer outros componentes internos do dispositivo deverão ser cobertos para reparo ou substituição sem custos adicionais.
- Atualizações e suporte ao software e firmware: Atualizações contínuas: O fornecimento de atualizações regulares e críticas de software e firmware, garantindo a segurança e a funcionalidade contínuas do equipamento.
- Entrega inicial: O software deverá ser entregue na versão mais recente e homologada pelo fabricante no momento da instalação.

- Suporte técnico ininterrupto (24/7): A contratada deverá fornecer atendimento técnico de forma ininterrupta, durante os 7 dias da semana, para suporte remoto e resolução de incidentes relacionados ao funcionamento do appliance.
- Conformidade e demais condições do edital: Garantir que todas as condições técnicas e funcionais estabelecidas no edital sejam atendidas.
- A solução deve ser amplamente documentada, com guias detalhados, especificações técnicas completas e suporte extensivo para implementação, configuração e manutenção. A documentação deve ser clara, acessível e atualizada, garantindo a facilidade de integração e operação.

#### Segurança Avançada,

- Recursos de NGIPS para prevenção de intrusões em tempo real.
- Suporte a NAT avançado (dinâmico, estático, bidirecional).
- Recursos IPv6: Dual Stack, NAT64, VPN SSL.

#### Funcionalidades Gerais,

- Sub-interfaces Ethernet Lógicas: Permitir criação e configuração de sub-interfaces para isolamento de tráfego e segmentação de redes.
- Roteadores Virtuais: Suporte para roteadores virtuais.
- Verificação de Rotas Estáticas e Alternativas: Implementar monitoramento de rotas estáticas e padrão, alternando para rotas secundárias em caso de falha.
- NAT Avançado: NAT dinâmico (Many-to-1 e Many-to-Many). NAT estático bidirecional (1-to-1). PAT (Port Address Translation). NAT de Origem/Destino simultâneos.

#### Suporte a Redes e VLANs,

- Suporte mínimo de 1000 VLAN Tags 802.1q.
- Agregação de Links com suporte ao protocolo 802.3ad e LACP.
- Encaminhamento Baseado em Política: Roteamento e balanceamento de carga.
- Servidor e Relay DHCP.
- Configuração de objetos de rede para interfaces de camada 3.

#### Recursos IPv6,

- Dual Stack IPv4/IPv6.
- NAT64 e suporte a SLAAC.
- Proteções contra DoS (Denial of Service/negação de serviço), Neighbor Discovery, e VPN SSL/IPSec em IPv6.

#### Segurança e Controle,

- Prevenção de Anti-Spoofing para evitar falsificação de endereços.
- Bloqueio de sessões TCP maliciosas (variações do 3-way handshake).
- Controle granular de aplicações e QoS baseado em usuários, portas e aplicações.
- LLDP e SNMP para mapeamento e troubleshooting de rede.
- Log detalhado com envio para sistemas externos via TCP/SSL, incluindo motivos de encerramento de sessões.



#### Modos de Operação,

- Sniffer (Monitoramento), L2 (Transparente), e L3 (Gateway): Operar em modos mistos com interfaces dedicadas a cada função.

#### Alta Disponibilidade,

- Suporte a configurações ativo/ativo e ativo/passivo em alta disponibilidade.
- Configuração de Ativo/Ativo e Ativo/Passivo: Sincronização de sessões, políticas, e VPNs. Alta disponibilidade em modos L2 e L3, com suporte a failover automático.

#### Desempenho e Compatibilidade,

- Garantia de funcionalidade sem contrato ativo de suporte ou atualização.
- Manutenção das capacidades: Firewall, IDS/IPS, controle de aplicações, VPN SSL/IPSec, QoS, NAT e VLANs.

#### Controle por Política de Firewall,

- Criação de Políticas Avançadas:
  - Controle baseado em: Zonas de segurança. Porta/protocolo. Aplicações, categorias e grupos (estáticos/dinâmicos). Endereços IP, redes e usuários (LDAP/AD).
  - Consulta a fontes externas para bloqueio/permissão de endereços IP, domínios e URLs.
  - Autenticação segura com certificados para acessar fontes externas de dados.
  - Gerenciamento e exceções via interface gráfica de administração.
  - Decriptografia e Controle SSL/TLS: Inspeção de tráfego inbound e outbound. Suporte a TLS 1.2, certificados ECC (ECDSA), e políticas específicas para SSH. Espelhamento de tráfego decriptografado para ferramentas externas (DLP, Forense, Análise de Ameaças).
  - Gestão Avançada de Tráfego: Bloqueio granular de tipos de arquivos (como .exe, .dll, etc.). Suporte completo para objetos IPv6 e regras multicast. Diferentes tipos de negação de tráfego: Drop sem notificação, ICMP Unreachable, ou TCP-Reset. Agendamento automático de políticas com base em horários predefinidos.
  - Reconhecimento Avançado de Aplicações: Detecção independente de portas e protocolos. Identificação heurística baseada em comportamento (ex.: BitTorrent, VoIP criptografado). Suporte para aplicações evasivas e criptografadas.
  - Decriptografia e Inspeção: Integração nativa para inspecionar tráfego SSL/TLS e leitura de payloads. Decodificação de protocolos para validar aplicações encapsuladas.
  - Gerenciamento Personalizado: Criação de assinaturas customizadas com expressões regulares. Controle sobre aplicações desconhecidas e comportamento anômalo. Criação de grupos dinâmicos com base em tecnologia, categoria e nível de risco. Alertas automáticos para o usuário em caso de bloqueio.
- Alta Disponibilidade: Modos Ativo/Passivo e Ativo/Ativo com sincronização de sessões, NAT, VPN e QoS. Operação contínua mesmo sem contrato ativo de suporte/software.

#### Módulos de Segurança Integrados,

- IPS (Sistema de Prevenção de Intrusão): Monitoramento contínuo com assinatura de bloqueio para exploits conhecidos e ataques de dia zero. Configuração de exceções específicas para fontes confiáveis. Ação configurável: bloquear, permitir com log, ou aplicar TCP-reset. Suporte à detecção de ataques DoS/DDoS com assinaturas específicas e bloqueio de buffer overflow.
- Proteção Contra Ameaças Digitais e Análises de Segurança: Possuir minimamente as funções existentes no modelo atualmente em uso pela CONTRATANTE: Anti Virus, Web Filter, DNS Filter/DNS Security, QoS, Application Control, Intrusion Prevention, File Filter, SSL/SSH Inspection, Application Signatures, IPS Signature, Categorização Personalizada de URLs/ Políticas Personalizadas de Filtragem Web. A CONTRATADA deve prover atualizações automáticas para manter as respectivas assinaturas atualizadas.

#### Configurações Granulares e Flexíveis,

- Regras Baseadas em Critérios Avançados: Definição de políticas por zona de segurança, endereço de origem/destino e serviço. Exceções configuráveis globalmente ou por assinatura. Regras específicas para detectar e bloquear tráfego HTTP/2.
- Ações por Detecção: Bloqueio direto do tráfego suspeito ou origem (IP do atacante). Logs detalhados para auditoria e resposta a incidentes.

#### Análise Avançada e Recursos Adicionais,

- Detecção de Protocolos Maliciosos: Decodificação para validar tráfego encapsulado. Identificação de ataques de encapsulamento DNS e comunicação de C&C.
- Logs Detalhados, registro de: Domínios suspeitos. ID da assinatura de detecção. IPs e usuários envolvidos. Severidade da ameaça e ações tomadas.

#### Alta Disponibilidade,

- Sincronização em configurações Ativo/Passivo e Ativo/Ativo para políticas de segurança e assinaturas. Operação contínua mesmo sem contrato de suporte/software.

#### Análise de Malware,

- Configuração por Tipo de Arquivo e Protocolo: Monitoramento de tráfego SMTP, POP3 e compartilhamento de arquivos. Inspeção de links em e-mails e relatórios detalhados sobre sites maliciosos ou phishing.
- Automação e Gerenciamento: Exportação de relatórios e resultados. Feedback direto para o fabricante sobre falsos positivos/negativos.

#### Filtro de URL,

- Políticas Baseadas em Grupos e Horários: Configuração de regras por usuários, grupos, IPs ou zonas de segurança. Definição de regras de filtro baseadas em categorias, URLs específicas e horários.
- Proteção contra Phishing e Roubo de Credenciais: Bloqueio de sites maliciosos com alertas ao usuário. Integração com LDAP ou Active Directory para políticas de acesso restritas.
- Classificação e Logs Detalhados: Suporte a classificação por nível de risco (baixo, médio e alto). Logs abrangentes com informações de cabeçalhos HTTP.
- Outras funções: Bloqueio ou filtro de URLs.

#### Identificação de Usuários,

- Autenticação e Controle: Integração com serviços de diretório como LDAP, Active Directory, e RADIUS. Captive Portal configurado para redes cabeadas e Wi-Fi, com suporte a Kerberos e SAML 2.0.
- Políticas Granulares por Usuários e Grupos: Criação de regras específicas para usuários identificados por x-forwarded-for. Monitoramento de múltiplos usuários conectados a um mesmo IP.
- Integração Específica: Deve permitir o gerenciamento de identidades e integração com controladoras wireless (de outros fabricantes).

#### Load balance,

- A solução de NGFW deverá incluir, de forma nativa ou complementar, funcionalidades de balanceamento de carga que permitam a distribuição eficiente do tráfego entre múltiplos links WAN e servidores internos. Essa funcionalidade deve permitir o balanceamento dinâmico dos links WAN com suporte a failover automático, roteamento baseado em políticas (policy-based routing) e otimização do tráfego com base em critérios como latência, largura de banda e disponibilidade. A solução deverá ainda permitir o balanceamento de carga entre servidores internos com base em critérios configuráveis. Também deverá permitir integração com diretórios corporativos, como o Active Directory, para tratamento diferenciado de tráfego, quando necessário. A solução deve prover visualização e monitoramento em tempo real do tráfego balanceado e suportar modos de alta disponibilidade, ativo/ativo ou ativo/passivo, assegurando a continuidade dos serviços em caso de falhas.

#### Web Application Firewall,

- A solução deverá incluir nativamente, ou como componente complementar devidamente integrado, um Web Application Firewall com funcionalidades de proteção avançada contra ameaças direcionadas a aplicações web. A solução deverá ser capaz de identificar e bloquear ataques como injeções de SQL, XSS (cross-site scripting), CSRF, e exploração de vulnerabilidades conhecidas, utilizando algoritmos de aprendizado de máquina e análise comportamental para detecção de padrões maliciosos. A solução deverá fornecer visibilidade centralizada sobre todo o tráfego de aplicações, independente de onde estejam hospedadas (nuvem, SaaS ou local), correlacionando eventos para alertas enriquecidos, priorização de risco e resposta automatizada a incidentes. Deve ainda incluir recomendações de endurecimento das configurações de segurança com base nos ataques identificados, bem como suporte a inspeção de tráfego criptografado SSL/TLS, mitigação de bots automatizados, análise de vulnerabilidades, e integração com fluxos de trabalho de resposta a incidentes. A proteção deverá abranger múltiplos ambientes de forma unificada, com gerenciamento por console centralizado, acessível via interface web segura.

#### Alta Disponibilidade,

- A solução de NGFW deverá permitir sincronização de configurações em Ativo/Passivo.

#### Licenciamento,

- As soluções propostas deverão considerar, no valor total do item 1, todos os custos relacionados às licenças necessárias para atender integralmente às especificações técnicas exigidas no edital. O período de vigência dessas licenças deverá ser equivalente ao prazo de garantia do equipamento, ou seja, 60 (sessenta) meses, assegurando a plena

operacionalidade, atualização e suporte contínuo da solução durante todo o período contratual, sem custos adicionais para a CONTRATANTE.

- Todas as licenças e produtos necessários para a execução dos requisitos técnicos deste item, incluindo aqueles voltados à compatibilidade, interoperabilidade e plena integração da solução, deverão ser, obrigatoriamente, do mesmo fabricante da solução de NGFW proposta, garantindo o correto funcionamento e suporte unificado do ambiente.

#### QUALIDADE DE SERVIÇO (QOS)

Controle de Tráfego e Políticas Personalizadas,

- Configurar políticas de controle baseadas em: Endereços de origem e destino. Usuários e grupos integrados com LDAP/AD. Aplicações específicas detectadas por inspeção de pacotes. Protocolos ou portas que consomem mais largura de banda.

Definição de Classes e Fila de Prioridade,

- Criar classes de tráfego, como: Alta prioridade: VOIP, videoconferência. Prioridade média: serviços corporativos (e.g., ERP, e-mails). Baixa prioridade: downloads grandes, tráfego de redes sociais.
- Alocar: Banda garantida: para serviços críticos. Banda máxima: limitar aplicações não críticas. Configurar filas de prioridade para priorizar pacotes sensíveis à latência.

Marcação Diffserv,

- Implementar marcações de pacotes (e.g., DSCP) para categorizar tráfego: EF (Expedited Forwarding): para VOIP e tráfego em tempo real. AF (Assured Forwarding): para aplicações corporativas importantes. BE (Best Effort): para tráfego geral.

Traffic Shaping e Estatísticas,

- Ativar traffic shaping para suavizar picos de tráfego em interfaces agregadas.
- Monitorar: Consumo por aplicação. Uso de largura de banda por classe. Estatísticas em tempo real para identificar gargalos.
- Permitir priorização de monitoramento de tráfego.

#### FILTRO DE DADOS

Criação de Filtros Personalizados,

- Configurar filtros para restringir tipos específicos de arquivos: Bloqueio de arquivos baseados em extensões (e.g., .exe, .zip, .docx). Prevenção de transferência de arquivos maliciosos ou não autorizados.
- Aplicar políticas específicas a arquivos compactados: Inspeccionar o conteúdo interno dos arquivos.

Identificação e Controle de Aplicações,

- Implementar uma lista abrangente de: Aplicações suportadas para controle. Tipos de arquivos compatíveis com o sistema de filtragem.

Monitoramento e Relatórios,

- Habilitar logs para rastrear: Tipos de arquivos bloqueados. Aplicações identificadas. Políticas aplicadas a cada tipo de tráfego.

Alta Disponibilidade e Integração,

- Sincronizar políticas e em modo ativo/passivo.

- Integração com serviços de diretório (LDAP/AD) para granularidade.

## VPN

### Suporte a Protocolos VPN,

- Habilitar suporte para os protocolos: IPsec VPN: Para conectividade segura entre sites (site-to-site). SSL VPN: Para acessos remotos seguros com ou sem agentes. Criptografia e Autenticação,
- A solução deve garantir suporte completo para autenticação multifatorial (MFA) integrada, com a possibilidade de implementar autenticação forte através de mecanismos como o uso de dispositivos móveis e OTP, atendendo aos requisitos mais exigentes de segurança.
- A solução deve fornecer o suporte para módulos de segurança de hardware (HSM) dedicados à proteção de chaves criptográficas, garantindo uma camada adicional de segurança para os dados transmitidos pela rede.
- Configurar algoritmos de criptografia robusta: AES-128, 192, 256. SHA-256 para integridade. Suporte a autenticação multifator (MFA) via Microsoft Authenticator.
- Implementar autenticação via: Certificados digitais (PKI). LDAP, RADIUS e SAML para autenticação centralizada.

### Integração com Protocolos de Autenticação,

- Configurar integração com: LDAP: Para validação de usuários/grupos. RADIUS: Para autenticação centralizada. SAML: Garantindo interoperabilidade com provedores de identidade (e.g., Azure AD).

### Segurança Avançada,

- Ativar recursos de firewall de próxima geração (NGFW) no tráfego VPN: Prevenção contra intrusões (IPS). Detecção e bloqueio de ameaças avançadas. Políticas de controle de aplicativos e filtragem de URL.

### Gerenciamento Centralizado,

- Utilizar interfaces de gestão centralizadas.

### Escalabilidade e Alta Disponibilidade,

- Implementar balanceamento de carga e failover: VPNs altamente escaláveis para milhares de conexões simultâneas. Configurações de alta disponibilidade (HA) para redundância.

### Monitoramento e Relatórios,

- Ativar ferramentas de monitoramento para: Estatísticas de tráfego por gateway e túnel. Relatórios detalhados de desempenho e eventos. Alertas de anomalias (integrados a sistemas SIEM).

### IPsec VPN: Detalhamento Técnico,

- Suporte a algoritmos de autenticação e criptografia: 3DES, AES (128, 192, 256), MD5, SHA-1/256. Grupos Diffie-Hellman (1, 2, 5, 14, etc.).
- Configurar IKEv1 e IKEv2 para tunelamento eficiente.
- Criar túneis site-to-site e client-to-site com: Regras de políticas adaptáveis para integração com roteamento dinâmico.

### SSL VPN: Configuração Específica,

- Permitir conexões via: Clientes dedicados (Windows, Linux). Interface web para dispositivos móveis.

- Suporte a: Atribuição dinâmica e estática de IP para usuários. Integração com políticas de segurança e visibilidade. Distribuição de certificados via portal centralizado.

Adicionais,

- Criar listas de bloqueio de dispositivos comprometidos ou provenientes de ataques de força bruta ou ataques de DoS (negação de serviço).
- Configurar mensagens customizadas para usuários sobre políticas ou expiração de senha.

Agente VPN SSL,

- Compatibilidade com Windows, macOS, Linux.
- Configurações específicas: Conexões antes e depois do login no sistema operacional. Acesso sob demanda, configurado por política central.

Portal VPN,

- Habilitar administração centralizada de gateways: Seleção automática de gateway com base em latência. Configuração de rotas baseadas em grupos LDAP.
- Implementar bloqueio de acesso externo/interno baseado em políticas.

#### ADERÊNCIA À REDES SD-WAN

- A solução SD-WAN proposta deverá ser completamente compatível com os mais altos padrões de criptografia e segurança, incluindo a implementação robusta de algoritmos como AES-256 e o protocolo IPsec.
- A solução deverá suportar os protocolos de rede e segurança amplamente utilizados no mercado, garantindo plena integração e interoperabilidade entre fabricantes distintos.

#### CERTIFICAÇÕES EXIGIDAS

Para garantir a segurança, qualidade e conformidade dos firewalls adquiridos, será exigido que o fabricante da solução possua as seguintes certificações: Common Criteria (EAL4+), FIPS 140-2 / 140-3, CyberRatings.org Recommended Rating e ISO/IEC 27001. Além disso, será exigido que a solução ofertada possua a seguinte certificação: Homologação Anatel. A seguir, essas certificações serão detalhadas e justificadas:

- 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.
- Certificação FIPS 140-2 / 140-3: Emitida pelo NIST, esta certificação garante que os produtos atendem aos requisitos de segurança para criptografia.
- Certificação ISO/IEC 27001: Embora essa certificação se refira aos sistemas de gestão de segurança da informação de uma organização, garantindo que seus processos de desenvolvimento e suporte atendem aos altos padrões de segurança.
- Certificação “CyberRatings.org Recommended Rating”: Garante que o firewall atenda aos mais altos padrões de segurança cibernética, com desempenho comprovado em testes independentes. Essa certificação assegura proteção eficaz contra ameaças, confiabilidade operacional e alinhamento com as melhores práticas do setor, reduzindo riscos e garantindo um investimento seguro para a administração pública.
- Homologação da Anatel: Equipamentos de firewall que incluem funcionalidades de roteamento ou conectividade sem fio devem ser homologados pela Anatel para garantir sua conformidade com as normas nacionais de telecomunicações e eletromagnéticas.

#### GARANTIA



- A garantia para o appliance de firewall deverá ser por um período mínimo de 60 (sessenta) meses, contados a partir da data de entrega e aceitação definitiva do equipamento pela ANM. Este período de garantia deve abranger todos os componentes do hardware, incluindo placa-mãe, processador, memória, disco rígido, fonte de alimentação e quaisquer outros componentes internos do dispositivo, firmware, entre outros.
- Caso o fabricante do equipamento forneça uma garantia ordinária inferior a 60 meses, será admitida a oferta de garantia estendida, contratada pelo fornecedor, para complementar o período restante, de modo a cumprir o total de 60 meses exigidos.
- A garantia, tanto ordinária quanto estendida, deverá assegurar a substituição ou reparo de qualquer componente defeituoso durante o período estipulado, sem custos adicionais para a ANM. Além disso, o fornecedor deverá comprometer-se a fornecer suporte técnico durante o período de garantia, incluindo assistência remota e acesso a atualizações de firmware e software necessárias para o funcionamento adequado do equipamento.

## **Item 2 - Console de gerenciamento de logs, análises e relatórios de ameaças de redes**

Características gerais (MÍNIMAS),

- O console de gerenciamento deve ser fornecido pelo mesmo fabricante do firewall, assegurando total compatibilidade e integração entre eles.
- Esse item será pago anualmente, a contar da data de assinatura do termo de recebimento definitivo da solução.
- Considerando este serviço fornecido pela solução ser **contínuo**, a vigência inicial do contrato será de 1 (um) ano, podendo ser prorrogada sucessivamente, desde que mantidas as condições vantajosas para a Administração, observando-se o prazo máximo estabelecido na Lei nº 14.133/2021. Caso a prorrogação não seja vantajosa ou necessária, a Administração poderá, sem ônus para as partes, negociar novos termos ou extinguir o contrato, garantindo a economicidade e a continuidade dos serviços essenciais de monitoramento e segurança da rede.
- É essencial que o console de gerenciamento seja disponibilizado preferencialmente como um serviço na nuvem (SaaS), garantindo acesso remoto conveniente, escalabilidade e atualizações automáticas. Essa abordagem proporciona flexibilidade operacional, permitindo que os usuários acessem e administrem o firewall de qualquer lugar, a qualquer momento, com facilidade. Contudo, caso o licitante não disponha de uma solução baseada em SaaS, será permitida a oferta de um appliance que atenda aos mesmos requisitos funcionais, desde que fornecido em regime de comodato ou por outra modalidade que não implique custos adicionais para a CONTRATANTE, ou, alternativamente, a disponibilização da solução em máquina virtual (VM), também em conformidade com os requisitos estabelecidos. Independentemente da forma de disponibilização, deverão ser incluídas, durante toda a vigência do serviço, todas as atualizações de software e licenciamento necessários para garantir a plena operacionalidade e segurança da solução, sem interrupções ou limitações.
- O console deve oferecer funcionalidades abrangentes, incluindo gerenciamento de logs, análises e relatórios de ameaças de rede, tudo a partir de uma única interface. Isso capacita a equipe da CONTRATANTE a gerenciar, automatizar, orquestrar e responder às ameaças, facilitando operações de segurança simplificadas, identificação proativa e remediação de riscos, com visibilidade completa da paisagem de ataques.

Funcionalidades Essenciais,

- Gerenciamento de Logs e Análises: O console deve fornecer ferramentas completas de gerenciamento de logs, análise e geração de relatórios de ameaças, tudo centralizado em uma interface única e intuitiva. Isso permitirá que a equipe de segurança da CONTRATANTE realize a orquestração, automação e resposta a incidentes de forma eficiente, proporcionando visibilidade abrangente da rede e identificando proativamente ameaças cibernéticas.

- **Análises e Relatórios Abrangentes:** O sistema deve permitir análises detalhadas de logs de eventos, riscos de segurança e comportamentos de rede em tempo real, proporcionando aos administradores insights profundos sobre a postura de segurança da rede. Os relatórios devem cobrir áreas cruciais, como segurança de VPN, conformidade, detecção de anomalias de rede e avaliações de ameaças cibernéticas, além de fornecer dados históricos para auditorias e conformidade regulatória.

Requisitos para a Solução de Gerenciamento de Firewall e Segurança,

- **Integração com Infraestrutura Existente:** A solução de gerenciamento do NGFW deve garantir total compatibilidade com a infraestrutura já implantada na instituição, incluindo cabeamento, switches core, solução de VoIP e Wi-Fi, assegurando a continuidade operacional sem necessidade de reconfigurações complexas ou substituição de equipamentos. Essa plataforma de gerenciamento deve permitir a administração eficiente e a automação de respostas a incidentes, garantindo a interoperabilidade com os sistemas e serviços em uso, sem impactar o desempenho ou a segurança da rede.
- **Visibilidade de Segurança e Relatórios Detalhados:** O console de gerenciamento deve permitir a geração de relatórios detalhados sobre postura de segurança, incluindo dados sobre ameaças cibernéticas, conformidade, avaliações de riscos, e incidentes de segurança. Ele deve fornecer insights acionáveis sobre as vulnerabilidades e atividades não autorizadas na rede.
- **Suporte a Políticas de Segurança Avançadas:** A solução de gerenciamento deve ser capaz de integrar autenticação multifatorial (MFA) por meio de protocolo SAML, para garantir interoperabilidade com provedores de identidade (p.ex. Azure AD), e para assegurar um controle de acesso robusto e seguro.

Licenciamento,

- As soluções propostas deverão considerar, no valor total do item 2, todos os custos relacionados às licenças necessárias para atender integralmente às especificações técnicas exigidas no edital.
- Todas as licenças e produtos necessários para a execução dos requisitos técnicos deste item, incluindo aqueles voltados à compatibilidade, interoperabilidade e plena integração da solução, deverão ser, obrigatoriamente, do mesmo fabricante da solução de NGFW proposta, garantindo o correto funcionamento e suporte unificado do ambiente.

### **Item 3 - Serviços de Instalação e Configuração de Firewall de Próxima Geração,**

Ao avaliar o escopo do serviço de instalação, os proponentes devem ter em mente que a ANM já possui um appliance de firewall instalado e operacional. Portanto, os serviços de instalação devem incluir, no mínimo, as seguintes etapas:

Reuniões Preliminares,

- Realização de reuniões de alinhamento para definir o escopo do projeto antes da instalação e apresentação do respectivo cronograma.

Instalação Física,

- Instalação física dos equipamentos (hardware) e licenças (softwares) adquiridos no local designado pela equipe responsável pelo projeto da contratante, incluindo considerações para instalação em modo de Alta Disponibilidade (ativo/passivo), se aplicável.

Análise da Rede Existente,

- Avaliação da topologia e arquitetura da rede, levando em conta todos os equipamentos existentes e instalados.

- Análise do acesso à Internet, sites remotos e serviços de rede oferecidos a funcionários e usuários externos.

#### Migração de Regras de Firewall,

- Migração das regras de firewall existentes e aplicáveis à nova solução, garantindo adequação às políticas de aplicações em camada 7 (também chamada camada de aplicação, é a camada mais alta no modelo OSI - *Open Systems Interconnection* - e lida com os aspectos específicos das aplicações de rede, como protocolos HTTP, FTP, SMTP e outros).

#### Análise de Perímetros de Segurança,

- Avaliação do posicionamento de outros equipamentos ou sistemas relevantes na segurança de qualquer perímetro protegido pela solução.

#### Configuração do Firewall,

- Configuração do sistema de firewall, VPN, IPS, Filtro URL, Anti-vírus e Anti-malware de acordo com os requisitos identificados.

#### Melhores Práticas e Ajustes,

- Realização de todas as configurações de sistema (políticas gerais, objetos, itens de administração) de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada.

#### Gerenciamento Centralizado,

- Configuração do sistema de gerenciamento centralizado, incluindo adição dos novos appliances.

#### Transferência de Conhecimento,

- 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,

- Documentação completa do processo de implantação, incluindo todas as configurações realizadas e decisões tomadas, em formato legível e tecnicamente fundamentado.

#### Certificação Técnica,

- Garantia de que os serviços sejam realizados por técnico certificado oficialmente pelo fabricante da solução ofertada ou pelo próprio fabricante.

#### Localização Física,

- Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local designado pela equipe responsável pelo projeto da contratante.

#### **Item 4 – Treinamento técnico especializado na solução de NGFW (uma turma),**

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.

#### **Item 5 – Operação assistida especializada prestada pelo fornecedor (HST),**

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.

#### Mensuração da Quantidade de Horas de Atendimentos,

- Para a operação assistida, será estabelecido um banco de horas anual, correspondente ao total de Horas de Serviço Técnico (HST) contratadas.
- 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.

## ANEXO B – NÍVEIS MÍNIMOS DE SERVIÇO (SLA)

O SLA (ou nível mínimo de serviço/NMS) relativo ao item 1 já se encontra detalhado no Termo de Referência.

O item 4 (treinamento) por ser de execução única não possui SLA relativo a ele.

Os itens 2, 3 e 5 estão submetidos aos níveis mínimos de serviço descritos a seguir:

- Na abertura de chamados técnicos serão fornecidas informações de identificação do produto, anormalidade observada, nome do responsável pela solicitação do serviço e severidade do chamado, conforme tabela sla1 a seguir:

Severidade	Situação	Início de Atendimento	Tempo máximo de solução	Expectativa
A	Impacto severo e/ou degradação total ou parcial do ambiente com aplicações críticas	Até 1 hora	3 horas	Solução definitiva ou temporária até a solução definitiva
B	Impacto moderado e/ou degradação parcial do ambiente com aplicações não críticas	Até 2 horas	6 horas	Solução de contorno e/ou temporária até a solução definitiva
C	Impacto mínimo e/ou degradação mínima do ambiente com aplicações não críticas	Até 48 horas	72 horas	Solução de contorno e/ou temporária até a solução definitiva

TABELA SLA1 – NÍVEIS DE SEVERIDADE

- Os níveis de severidade são aplicados ao objeto do Termo de Referência.
- Caso não seja possível, em virtude da complexidade, pendências da CONTRATANTE ou motivo de força maior, não seja possível concluir o atendimento dentro dos prazos máximos de solução estipulados, a CONTRATADA deverá, antes da expiração do tempo máximo de solução, solicitar a extensão deste prazo.
- O atendimento aos chamados classificados com severidade A não poderá ser interrompido até o completo restabelecimento do serviço, mesmo que se estenda além do horário comercial, seja ele noturno, ou finais de semana e feriados. A interrupção do atendimento por parte da CONTRATADA na qual a CONTRATANTE não esteja de acordo, poderá ensejar na aplicação das sanções previstas.
- Os chamados classificados com severidade B, quando não solucionados no prazo definido, poderão ser escalados para a severidade A, sendo que os prazos de atendimento e solução bem como as sanções previstas são devidamente ajustadas para o novo nível.
- Por excepcionalidade a CONTRATANTE poderá solicitar a alteração da severidade do chamado para níveis superiores ou inferiores de severidade. Nesse caso, a mudança deverá ser justificada e os prazos dos chamados passarão a contar do início novamente.
- Os chamados, quando possível, poderão ser analisados e solucionados remotamente. Entretanto, aqueles classificados com níveis de severidade A, preferencialmente deverão ser solucionados por intermédio de suporte on-site.
- Todos os chamados efetuados receberão uma identificação e serão controlados pela CONTRATANTE em ferramenta própria.



- O encerramento dos chamados sem a devida solução, em qualquer nível de severidade, e sem a prévia concordância por parte CONTRATANTE, serão reabertos e os prazos serão contados a partir da data de abertura inicial dos chamados, inclusive para efeito de aplicação das sanções previstas.
- A CONTRATANTE informará previamente a relação de pessoas que poderão efetuar a abertura e o fechamento dos chamados em nome desta.
- Sempre que os tempos de início do efetivo de atendimento e de solução não forem cumpridos, bem como surgir qualquer outra situação irregular, a CONTRATANTE irá notificar a CONTRATADA de tal fato, para que a mesma tome as devidas providências.
- A CONTRATADA será eximida de qualquer penalidade quanto ao não atendimento dos tempos de solução, desde que comprovadas às seguintes situações:
  - Quando constatado que o problema está relacionado a “bug” no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio.
  - Que a CONTRATADA tomou todas as medidas possíveis visando providenciar a solução de contorno.
  - O não cumprimento dos níveis mínimos exigidos ensejará em glosas, de acordo com o descrito abaixo.
  - Para as Ordens de Serviço ou chamados classificados com nível de severidade A, glosas serão aplicadas conforme tabela sla2:

ID	OCORRÊNCIA	GLOSA
1	Deixar de atender chamado técnico	0,5 % sobre o valor a ser pago.
2	Reabertura de chamado técnico por falha no atendimento.	0,5 % sobre o valor a ser pago.
3	Exceder o limite para início de atendimento	0,5 % sobre o valor a ser pago, mais 0,1 % por hora excedente sobre o valor da Ordem de Serviço, por ocorrência, limitando-se a 15%
4	Ultrapassar o limite máximo de tempo para solução	0,5 % sobre o valor a ser pago, , limitando-se a 5%.

**TABELA SLA2 – SEVERIDADE A**

- Para as Ordens de Serviço ou chamados classificados com nível de severidade B, a Tabela de Glosas a seguir será aplicada (tabela sla3):

ID	OCORRÊNCIA	GLOSA
1	Deixar de atender chamado técnico	0,2 % sobre o valor o valor a ser pago, por ocorrência.
2	Reabertura de chamado técnico por falha no atendimento.	0,2 % sobre o valor o valor a ser pago, por ocorrência.
3	Exceder o limite para início de atendimento	0,2% sobre o valor a ser pago, limitando-se a 2,4%
4	Ultrapassar o limite máximo de tempo para solução	0,2% sobre o valor a ser pago, limitando-se a 2,4%

**TABELA SLA3 – SEVERIDADE B**

- Para as Ordens de Serviço ou chamados classificados com nível de severidade C, a Tabela de Glosas a seguir será aplicada (tabela sla4):

ID	OCORRÊNCIA	GLOSA
1	Deixar de atender chamado técnico	0,1 % sobre o valor o valor a ser pago, por ocorrência.
2	Reabertura de chamado técnico por falha no atendimento.	0,1 % sobre o valor o valor a ser pago, por ocorrência.
3	Exceder o limite para início de atendimento	0,1% sobre o valor a ser pago, limitando-se a 1,0%
4	Ultrapassar o limite máximo de tempo para solução	0,1% sobre o valor a ser pago, limitando-se a 1,0%

**TABELA SLA4 – SEVERIDADE C**

## **ANEXO C – INFORMAÇÕES COMPLEMENTARES SOBRE O MODELO DE EXECUÇÃO DO CONTRATO**

### **DA EXECUÇÃO GERAL DOS SERVIÇOS PREVISTOS NO OBJETO,**

- Os serviços e os produtos serão entregues na sede da ANM em Brasília-DF.
- Os serviços objeto desta licitação serão executados preferencialmente na modalidade de teletrabalho (trabalho remoto), no entanto, a critério da ANM, poderão ser solicitados que serviços sejam realizados nas dependências da CONTRATADA, mediante comunicação prévia.
- Os serviços serão realizados conforme escopo e prazos definidos nas OS (ordem de serviço) quando couber, cabendo ao Gerente de Projetos o controle do timesheet da equipe, que poderá ser auditado pelo gestor do contrato se julgar pertinente.
- Os meios físicos e lógicos para execução do objeto deverão ser providos pela CONTRATADA à sua equipe técnica, devendo sempre se adequar às especificidades das demandas e normativas da CONTRATANTE (p. ex. POSIC, padrão de comunicação, ferramentas, etc...).
- Os serviços serão solicitados via emissão de ordens de serviço (OS) registradas na ferramenta de acompanhamento da CONTRATANTE, ou abertura de chamado quando se tratar de demanda do item 5.
- A CONTRATANTE definirá o modelo da OS.
- A critério da CONTRATANTE o modelo de Ordem de Serviço poderá ser alterado para atender as necessidades do serviço, sem criar qualquer obrigação adicional à CONTRATADA, devendo, contudo, manter as informações mínimas necessárias para sua execução (cita-se escopo, não escopo, data de início e de fim, necessários à respectiva execução, valores, entregáveis e requisitos de aceitação).
- A CONTRATANTE é a responsável pela definição do escopo da OS.
- Todas as OS deverão ser assinadas por ambas as partes.
- Havendo, por parte da CONTRATADA, alguma divergência na OS, desde que haja justificativa fundamentada, poderá a CONTRATANTE analisar e conduzir a solução das divergências e reapresentar a OS.
- As OS poderão sofrer ajustes (decorrentes de situações supervenientes ocorridas na sua execução, que impliquem eventualmente na revisão de prazos, custos ou escopo), sempre formalizados por meio de Relatórios de Impacto (RI), assinados por ambas as partes, desde que não tenha sido dado o aceite definitivo nas respectivas entregas. A aceitação dos serviços é baseada na verificação dos entregáveis aferíveis preestabelecidos, conforme preconizado na Súmula TCU Nº 269 e no Acórdão Nº

916/2015 – Plenário – TCU. Este RI e os respectivos impactos nas OS deverão ser registrados na Ferramenta de Acompanhamento da CONTRATANTE.

- O pagamento das Ordens de Serviço será função não somente do escopo executado, mas também do alcance de níveis de serviço em cada entrega, que considerarão critérios de prazo e qualidade (NMS/SLA).
- O dimensionamento da equipe para execução adequada do serviço contratado é de responsabilidade exclusiva da CONTRATADA, devendo ser suficiente para o cumprimento integral dos prazos, da qualidade e dos níveis de serviço exigidos.
- A eventual suspensão ou cancelamento da OS pela CONTRATANTE implicará na remuneração proporcional de fases entregues e aceitas definitivamente até esse momento, nesta situação também é necessária a emissão e assinatura do respectivo relatório de impacto (RI).
- A execução das Ordens de Serviço pela Contratada ocorrerá de acordo com as condições, processos e atividades estabelecidos nesse Termo de Referência e anexos.
- A CONTRATANTE pode, contudo, a seu critério, na abertura da OS, estabelecer condições específicas de fornecimento respeitando os limites estabelecidos no Termo de Referência.
- A entrega dos artefatos e subprodutos da OS é realizada desde seu início até seu término, em consonância com as fases do processo e a produção dos produtos.
- A entrega em caráter provisório (aceite provisório) se dará por meio do registro eletrônico na ferramenta de acompanhamento da CONTRATANTE.
- A entrega em caráter definitivo (aceite definitivo) se dará por meio do registro eletrônico na ferramenta de acompanhamento da CONTRATANTE e seus respectivos artefatos (na forma definida pela CONTRATANTE) e da emissão e assinatura do Termo de Recebimento Definitivo (TRD) por ambas as partes.
- O modus operandi das reuniões relativas à metodologia relativa à execução do objeto serão definidas pela CONTRATANTE e repassadas formalmente à CONTRATADA, podendo sofrer ajustes durante a execução do objeto e vigência do contrato.
- A CONTRATANTE poderá, sempre que julgar necessário, com emissão do respectivo RI, promover a alteração/atualização/supressão de escopo das Ordens de Serviços pela CONTRATANTE. Nessas situações, será feita avaliação de impacto estabelecendo, quando necessário, as novas condições de fornecimento.
- A CONTRATADA registrará as entregas dos produtos na Ferramenta de Acompanhamento da CONTRATANTE, primeiro de forma provisória, contando a data de entrega dos artefatos como sendo a entrega provisória.

- O aceite definitivo dos serviços é emitido apenas após o atendimento das condições gerais e específicas dos serviços contratados, conforme estabelecido nesse Termo de Referência, sendo emitido para tal o Termo de Recebimento Definitivo (TRD) para a OS.
- A critério exclusivo da CONTRATANTE, uma OS poderá ser finalizada pela CONTRATADA com a entrega parcial dos serviços e/ou artefatos solicitados na OS. Nesse caso os itens faltantes podem vir a ser executados em outra OS, sendo que os tamanhos das entregas afetadas deverão ser recalculados, refletindo-se os novos valores obtidos de prazo e valor da OS.