Termo de Referência 19/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
19/2024	130005-COORD.-GERAL DE EXECUCAO ORç.E FIN. /DA/MAPA	THIAGO PEREIRA DA COSTA	14/03/2024 14:31 (v 3.0)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Bens de TIC		21000.020025/2023-02

1. Definição do objeto

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1 - Contratação de empresa para o fornecimento de solução de proteção de rede "Next Generation Firewall", contemplando os hardwares ,licenciamento, instalação, configuração, solução de armazenamento de logs e relatoria, Solução para gerenciamento centralizado dos equipamentos, treinamento, ZTNA, garantia e suporte técnico por 60 meses, de acordo com as condições, exigências, especificações e quantidades constantes deste termo de referência e seus Anexos.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QTDE	VALOR UNITÁRIO	VALOR TOTAL
01	Firewall - Solução de plataforma de segurança denominada Next Generation Firewall (NGFW) com instalação, suporte, garantia e licenciamento inclusos.	484747	UNIDADE	0 4 Unidades	R$ 1.306.986,00	R$ 5.227.944,00
02	Solução de armazenamento de logs e relatoria, com instalação, suporte, garantia e licenciamento inclusos.	481647	UNIDADE	0 1 unidade	R$ 126.480,86	R$ 126.480,86
03	Solução para gerenciamento centralizado dos equipamentos, com instalação, suporte, garantia e licenciamento inclusos.	481647 /27472	UNIDADE	0 1 unidade	R$ 103.007,54	R$ 103.007,54
04	Treinamento ministrado por profissional certificado pelo fabricante.	16837	CAPACITAÇÃO	01 turma	R$ 43.662,61	R$ 43.662,61
	Plataforma de ZTNA - Zero Trust Network					

05	Access, com instalação, suporte, garantia e licenciamento inclusos.	27742	SERVIÇO	0 1 unidade	R$ 782.666,67	R$ 782.666,67

1.2 - O objeto desta contratação faz parte dos catálogos de soluções de TIC aos quais possuem condições não padrões definidas pelo Órgão Central do SISP conforme destacado no link " https://www.gov.br/governodigital/pt-br/contratacoes /catalogo-desolucoes-de-tic". Por isso, não é necessário preenchimento da coluna "cód. PMC-TIC" do modelo de TR da AGU.
1.3 - Todos os bens e serviços desta contratação são caracterizados como comuns, pois possuem padrões de desempenho e qualidade objetivamente definidos pelo edital, por meio de especificações usuais no mercado. Além disso, o objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto Nº 10.818, de 27 de Setembro de 2021.
1.4 - O objeto da presente contratação não incide na hipótese do inciso II do artigo 3º da IN SGD/ME nº 94, de 23 de dezembro de 2022. Ademais, a contratação em tela não pode ser integrada à plataforma de cidadania digital, nos termos do decreto Nº 8936, de 19 de dezembro de 2016, pois não está relacionada à oferta digital de serviços públicos.

1.5. - O prazo de vigência contratual será de 60 meses, contados a partir da data de assinatura do contrato, na forma do artigo 105 da Lei Nº 14.133, de 2021.

1.6 - O contrato oferecerá maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. Fundamentação da contratação

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1 - VISÃO GERAL DO MINISTÉRIO DA AGRICULTURA E PECUÁRIA-MAPA
O Ministério da Agricultura e Pecuária (MAPA) é responsável pela gestão das políticas públicas de estímulo à agropecuária, pelo fomento do agronegócio e pela regulação e normatização de serviços vinculados ao setor. No Brasil, o agronegócio contempla o pequeno, o médio e o grande produtor rural e reúne atividades de fornecimento de bens e serviços à agricultura, produção agropecuária, processamento, transformação e distribuição de produtos de origem agropecuária até o consumidor final. Além
disso, O MAPA tem como missão promover o desenvolvimento sustentável das cadeias produtivas agropecuárias, em benefício da sociedade brasileira.

O Ministério da Agricultura e Pecuária- MAPA, órgão da administração pública federal, tem, dentre outras, as competências para atuar nos seguintes temas abaixo:

- Política agrícola, abrangidos a produção, a comercialização e o seguro rural.
- Produção e fomento agropecuário, abrangidas a agricultura, a pecuária, a agroindústria, a agroenergia, a heveicultura e, em articulação com o Ministério do Meio Ambiente e Mudança do Clima, as florestas plantadas.
- Informação agropecuária.
- Defesa agropecuária e segurança do alimento.
- Pesquisa em agricultura, pecuária, sistemas agroflorestais, aquicultura e agroindústria; Conservação e proteção de recursos genéticos de interesse para a agropecuária e a alimentação; Assistência técnica e extensão rural.
- Irrigação e infraestrutura hídrica para a produção agropecuária, observadas as competências do Ministério da Integração e do Desenvolvimento Regional.
- Informação meteorológica e climatológica para uso na agropecuária; Desenvolvimento rural sustentável.
- Conservação e manejo do solo e da água, destinados ao processo produtivo agrícola e pecuário e aos sistemas agroflorestais; Boas práticas agropecuárias e bem-estar animal.
- Cooperativismo e associativismo na agropecuária.
- Energização rural e agroenergia, incluída a eletrificação rural e
- Negociações internacionais relativas aos temas de interesse das cadeias de valor da agropecuária.

Atualmente, O MAPA é composto de várias unidades em sua estrutura:

- Órgãos de assistência direta e imediata ao Ministro de Estado da Agricultura e Pecuária (Gabinete, assessorias especiais, ouvidoria, corregedoria, consultoria jurídica e secretaria executiva).
- Órgãos específicos singulares (Secretaria de Política Agrícola, Secretaria de Defesa Agropecuária, Secretaria de Inovação, Desenvolvimento Sustentável, Irrigação e Cooperativismo e Secretaria de Comércio e Relações Internacionais).
- Unidades descentralizadas (Superintendências de Agricultura e Pecuária).

- Órgãos colegiados (Comitê Gestor Interministerial do Seguro Rural, Comissão Coordenadora da Criação do Cavalo Nacional, Comissão Especial de Recursos, Conselho Deliberativo da Política do Café, Conselho Nacional de Política Agrícola; e Comitê Estratégico do Programa Nacional de Levantamento e Interpretação de Solos do Brasil).
- Entidade Vinculada (Empresa Brasileira de Pesquisa Agropecuária - Embrapa).

Além das citadas, o MAPA ainda provê infraestrutura para o INMET E CONAB, como é o caso do sistema SEI. Conforme evidenciado, a estrutura do Ministério da Agricultura, Pecuária e Abastecimento (MAPA) é notavelmente vasta e intricada, abrangendo diversas esferas de atuação que requerem tratamento individualizado, alinhado não apenas com as suas dimensões, mas também com o nível de sensibilidade e sigilo inerentes às atividades desempenhadas em cada área.
Para viabilizar a operação eficaz de todos os órgãos que compõem a estrutura ministerial e assegurar os recursos necessários para a plena execução de suas funções, é essencial contar com soluções tecnológicas capazes de agregar valor e disponibilizar as informações requeridas. Isso possibilitará a geração oportuna de conhecimento, facilitando a tomada de decisões em todos os níveis, incluindo estratégico, tático e operacional.
Com a Medida Provisória Nº 1.154, de 1º de janeiro de 2023, o compartilhamento de atividades de administração patrimonial, de material, de gestão de pessoas, de serviços gerais, de orçamento e finanças, de contabilidade, de logística, de contratos, de tecnologia da informação, de planejamento governamental e gestão estratégica e de outras atividades de suporte administrativo deve ser realizada por meio de arranjos colaborativos entre Ministérios ou modelos centralizados, por isso essa contratação também irá atender os Ministérios da Pesca e Aquicultura-MPA e Ministério do Desenvolvimento Agrário e Agricultura Familiar-MDA. As despesas executadas para a prestação de serviços administrativos compartilhados serão assumidas pelo Ministério demandante, sem necessidade de celebração de termo de execução descentralizada, nos termos do inciso II do § 3º do art. 3º do Decreto nº 10.426, de 16 de julho de 2020.

2.2 . ALINHAMENTO DA SOLUÇÃO DE TIC COM OS INSTRUMENTOS DE PLANEJAMENTO

2.2.1. - CONTEXTUALIZAÇÃO

Os constantes ataques cibernéticos, a necessidade de continuidade do negócio e a evolução de ameaças das mais variadas espécies criam a necessidade de contratação de uma solução eficaz que proteja as informações dos órgãos públicos (MAPA e Ministérios demandantes) e diminua os riscos de acesso indevido às mesmas. Essa crescente disseminação de ataques, em especial à Administração Pública, vem sendo alvo de ações maliciosas com destaque para invasões de sites oficiais, indisponibilidade de recursos e serviços, exposição de vulnerabilidades e consequentes vazamentos de informações, causando assim prejuízos não só ao erário, mas também reflexos negativos no atendimento aos cidadãos , empresas e demais entes envolvidos.
Devido ao aumento significativo dessas ameaças, é imprescindível implementar inteligência e automatização no gerenciamento das soluções de segurança. As ferramentas adotadas para o cenário de outrora tornaram-se insuficientes, uma vez que as tecnologias de mercado evoluíram e o ambiente se expandiu consistentemente. Assim, é prudente acompanhar a evolução e adotar as atualizações tecnológicas necessárias para fornecer serviços adequados e mais seguros. Além disso, em um contexto dinâmico de constante evolução tecnológica e em um curto intervalo de tempo, os equipamentos destinados à segurança da informação podem se tornar obsoletos a tal ponto de não suportarem o aumento do tráfego de internet e dados, o crescimento de novos usuários/novas ameaças e tentativas de invasões das redes corporativas. As tecnologias voltadas à segurança da informação estão em constante evolução, e os fabricantes buscam soluções eficazes para obter o melhor desempenho dos firewalls e ao mesmo tempo prover inteligência proativa, reunindo as mais diversas funcionalidades.
À medida que a dependência do MAPA por sistemas e serviços de informação aumenta, crescem também as ameaças cibernéticas que, muitas vezes, resultam em falhas de segurança críticas que, por sua vez, podem gerar centenas de milhões de reais de prejuízo aos cidadãos, além de causar grandes danos à imagem dos Ministérios (provedor e demandantes). Nesse sentido, a adoção de tecnologias modernas e inovadoras, como solução de firewall do tipo "next generation firewall" de alto desempenho, deixaram de ser uma tendência e passaram a ser uma realidade na administração pública federal, que deve estar alinhada às modernas e eficientes práticas do mercado. Os firewalls possuem funções fundamentais em uma rede de TIC, podendo evitar que os pacotes indesejados e prejudiciais tenham acesso à rede interna, e portanto, às informações e recursos em posse da mesma.
O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) responsável por coordenar as atividades de segurança da informação e das comunicações no governo federal, em sua portaria GSI/PR Nº 120, de 21 de Dezembro de 2022 (https://www.in.gov.br/en /web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918) deixa claro as orientações para proteção das entidades publicas do executivo federal, ao qual destacamos:

2. PREVENÇÃO

A prevenção é um processo constante de ações proativas com o objetivo de reduzir a probabilidade de ataques cibernéticos bem-sucedidos. Entre essas ações, enfatizam-se as de definição e de implementação de controles de segurança, de gerenciamento de vulnerabilidades, de conscientização e de capacitação.

As ações preventivas de segurança cibernética deverão contemplar aquelas previstas na política de segurança da informação do integrante da Regic.

2.1. Definição e implementação de controles de segurança preventivos

Os controles de segurança preventivos constituem-se em tecnológicos, organizacionais e físicos.

Os controles tecnológicos são aqueles utilizados para reduzir vulnerabilidades no **hardware** e no **software**. Entre os principais de controles tecnológicos estão:

- dispositivos **endpoint** do usuário;
- restrição de acesso à informação;
- autenticação segura;
- proteção contra **malware**;
- **backup** das informações;
- atividades de monitoramento (log);
- segurança de redes;
- uso de criptografia; e
- gestão de mudanças.

Ainda com relação à portaria citada acima, os controles físicos tem por finalidade prevenir ou evitar o acesso não autorizado à área ou material sensível, bem como os danos e interferências às áreas que contenham informações críticas ou sensíveis. Entre os principais controles físicos estão:

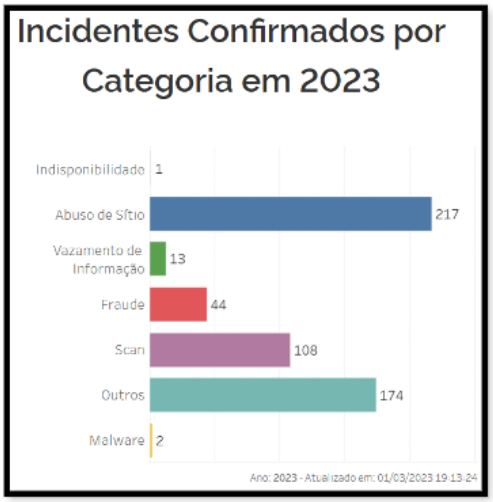
- Definição dos perímetros de segurança física.
- Monitoramento de segurança física.
- Proteção contra ameaças físicas e ambientais.
- Localização e proteção de equipamentos.
- Segurança de ativos fora das instalações da organização e Manutenção dos ativos.

Ainda nesta linha o Centro de Prevenção , Tratamento e Resposta a Incidentes Cibernéticos de Governo, entidade que está enquadrada na categoria "CSIRT de responsabilidade nacional de coordenação" publica regularmente relatórios sobre a quantidade de incidentes descobertos (https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/visao-geral) . Vejamos alguns dados importantes:

2019	2020	2021	2022	2023
23.674	24.300	22.298	18.489	3.254
10.716	5.257	4.910	3.786	559
1.201	2.270	3.917	3.189	680

Atualizado em: 01/03/2023 19:13:24

Notificações Incidentes Vulnerabilidades



Percebe-se que a quantidade de incidentes no âmbito do governo federal é extremamente relevante. Em relação à proteção de perímetro, temos que esta é uma das proteções mais importantes em uma instituição, e que se atualizam constantemente por meio de soluções que são conhecidas, atualmente, no mercado como NGFW.

2.2.2 . DESCRIÇÃO DA NECESSIDADE

A aquisição de uma nova solução de firewall do tipo Next-Generation Firewall (NGFW) pode trazer vários benefícios para uma organização. Entre elas:

- Proteção avançada contra ameaças: Um NGFW oferece recursos de segurança avançados que podem proteger contra ameaças cibernéticas, como malware, phishing, ransomware e ataques de dia zero. Isso inclui recursos como detecção de intrusões, filtragem de URL, antivírus, inspeção de tráfego SSL/TLS e muito mais.
- Controle de acesso a aplicativos: Um NGFW permite que uma organização controle o acesso a aplicativos específicos, permitindo ou bloqueando o acesso com base em políticas de segurança definidas. Isso ajuda a proteger contra o uso indevido de aplicativos e reduz o risco de violações de dados.
- Visibilidade e controle de tráfego: Um NGFW fornece uma visão completa do tráfego de rede, permitindo que as organizações monitorem e controlem o tráfego de entrada e saída. Isso pode ajudar a identificar e mitigar atividades suspeitas e proteger contra vazamentos de dados.
- Gerenciamento centralizado: Um NGFW pode ser gerenciado de forma centralizada, permitindo que as organizações gerenciem políticas de segurança, implementem atualizações e monitorem o tráfego de rede em vários locais a partir de um único console.

Quanto à inclusão do item Zero Trust Network Access-ZTNA na contratação, seguem os motivos:

As VPNs tem sido uma solução confiável por muito tempo e continuam desempenhando um papel importante na conectividade remota e segura aos colaboradores do MAPA. Entretanto, elas não foram projetadas para uso em ambientes altamente distribuídos como hoje, pois as aplicações e sistemas não estão mais concentradas no datacenter, e sim em multinuvem /ambientes híbridos.

Desta forma, a rápida mudança para o trabalho remoto e híbrido, juntamente ao rápido aumento nas adoções da nuvem combinada, evidenciou-se que essa abordagem tradicional de segurança baseada em perímetro tem se tornado ineficaz com as técnicas mais avançadas de hacking.

No ambiente computacional híbrido e de várias nuvens públicas, o uso de VPN enfrenta algumas desvantagens, tais como:

- Segurança Baseada em Perímetro: As VPNs operam com base na confiança no perímetro da rede, o que pode ser inadequado para proteger contra ameaças internas e externas.
- Acesso Amplo: As VPNs geralmente fornecem um acesso amplo à rede interna, muitas vezes concedendo mais permissões do que o necessário a todos os usuários.
- Complexidade de Gerenciamento: À medida que as redes se tornam mais complexas, o gerenciamento de VPNs e a garantia de conformidade de segurança podem se tornar desafiadores.
- Problema na verificação contínua do tráfego.

Desta forma, com a evolução das necessidades de segurança e as complexidades desses ambientes em diversas nuvens públicas e maior número de pessoas trabalhando fora do MAPA, surgiu uma alternativa mais moderna conhecida como ZTNA (Zero Trust Network Access), que apresenta várias vantagens em relação às VPNs tradicionais.

A autenticação baseada em identidade e o controle de acesso encontrados nos serviços ZTNA fornecem uma alternativa ao controle de acesso baseado em IP, normalmente usado com a maioria das configurações de VPN que ajudam a reduzir a superfície de ataque de uma organização. A ZTNA também permite que as organizações implementem políticas de controle de acesso específicas de localização ou dispositivo para evitar que dispositivos vulneráveis se conectem a serviços corporativos.

Desta maneira, isso alivia os desafios comuns relacionados à VPN, em que os usuários remotos BYOD recebem o mesmo nível de acesso que os usuários em um escritório físico do MAPA, apesar de muitas vezes terem menos controles de segurança em vigor. Abaixo, seguem algumas características/benefícios do ZTNA:

- Princípio de confiança Zero: O ZTNA não pressupõe confiança baseada em perímetro e aplica uma mentalidade de "nunca confiar, sempre verificar" em relação a todos os dispositivos e usuários, mesmo aqueles dentro da rede interna.
- Acesso Baseado em Políticas: O ZTNA concede acesso com base em políticas granulares, fornecendo permissões específicas necessárias para tarefas específicas.
- Verificação contínua de confiança: Depois que o acesso a um aplicativo é concedido, a confiança é avaliada continuamente com base nas mudanças na postura do dispositivo, no comportamento do usuário e no comportamento do aplicativo. Caso seja detectado algum comportamento suspeito, o acesso pode ser revogado em tempo real.
- Inspeção de segurança contínua: A inspeção profunda e contínua é realizada em todo o tráfego, mesmo nas conexões permitidas, para evitar todas as ameaças, incluindo ameaças de dia zero. Isto é especialmente importante em cenários em que credenciais legítimas de usuários são roubadas e usadas para lançar ataques contra aplicativos ou infraestrutura.
- Segmentação Lógica da Rede: Ele permite a segmentação lógica da rede, isolando os recursos de acordo com sua sensibilidade e o princípio do menor privilégio.
- Redução de Super privilégios: O ZTNA reduz a probabilidade de super privilégios concedidos por meio de VPNs tradicionais, limitando o acesso estritamente ao que é necessário.

- Facilidade de Gerenciamento/Eficiência Operacional: Com políticas granulares, o gerenciamento de políticas e conformidade é simplificado, proporcionando maior visibilidade e controle, consequentemente, melhorando a eficiência operacional.
- Segurança Reforçada: O ZTNA reduz o risco de comprometimento da rede e protege contra ameaças internas e externas.
- Conformidade: O ZTNA facilita o cumprimento de regulamentações de segurança e privacidade.
- Adoção de Nuvens Públicas: Facilita a migração para ambientes de várias nuvens públicas, mantendo a segurança e a conformidade.
- Acessibilidade Segura: Oferece acesso seguro a partir de qualquer local, mantendo as operações ininterruptas.

Em resumo, embora as VPNs tenham sido uma solução confiável na medida do possível, o ambiente computacional atual e as crescentes ameaças exigem uma abordagem mais moderna e flexível como o ZTNA. A transição para o ZTNA pode proporcionar uma segurança aprimorada, gerenciamento simplificado e maior eficiência operacional, tornando-o uma escolha sólida para o MAPA e organizações de todos os setores.
Dentro do contexto analisado, a substituição da solução de TIC relacionada ao firewall do MAPA e demais Ministérios demandantes (MPA e MDA) é essencial, uma vez que regula o tráfego de dados entre redes distintas e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede, além de trazer outros inúmeros benefícios que serão detalhados ao longo do estudo técnico preliminar quanto no termo de referência.
Por fim, resumidamente, a necessidade da contratação engloba aquisição de solução de proteção de rede "Next Generation Firewall", contemplando os hardwares ,licenciamento, implantação, configuração, solução de armazenamento de logs e relatoria, Solução para gerenciamento centralizado dos equipamentos, treinamento, ZTNA, garantia e suporte técnico por 60 meses.

2.3 . ALINHAMENTO DA SOLUÇÃO DE TIC COM OS INSTRUMENTOS DE PLANEJAMENTO

2.3.1. - ALINHAMENTO AO PCA 2024

Número da contratação	Título da contratação	Valor total da contratação	Data estimada para a conclusão do processo de contratação	Prioridade	Data da conclusão da Contratação no DFD	Classificação da Contratação	Descrição material/serviço	Unidade Fornecimento	Valor Unitário	Quantidade	Valor Total
jun/24	Aquisição de equipamentos Firewall do tipo Next Generation Firewall(NGFW)""	R$ 6.792.000,00	01/07/2024	Médio	01/07/2024	Material	APLICAÇÃO:	UN	R$ 1.400.000,00	4	R$ 5.600.000,00
jun/24	Aquisição de equipamentos Firewall do tipo Next Generation Firewall(NGFW)""	R$ 6.792.000,00	01/07/2024	Médio	01/07/2024	Material	APLICAÇÃO:	UN	R$ 150.000,00	1	R$ 150.000,00
jun/24	Aquisição de equipamentos Firewall do tipo Next Generation Firewall(NGFW)""	R$ 6.792.000,00	01/07/2024	Médio	01/07/2024	Material	APLICAÇÃO:	UN	R$ 120.000,00	1	R$ 120.000,00
jun/24	Aquisição de equipamentos Firewall do tipo Next Generation Firewall(NGFW)""	R$ 6.792.000,00	01/07/2024	Médio	01/07/2024	Serviço	TREINAMENTO INFORMÁT	R$ 72.000,00	1	R$ 72.000,00
jun/24	Aquisição de equipamentos Firewall do tipo Next Generation Firewall(NGFW)""	R$ 6.792.000,00	01/07/2024	Médio	01/07/2024	Serviço	LICENCIAMENTO DE DIRE	R$ 850.000,00	1	R$ 850.000,00

2.3.2 -ALINHAMENTO AO PDTIC 2021-2031/PLANEJAMENTO ESTRATÉGICO DO MAPA

META 7	NECESSIDADE 5	INDICADOR	OBJETIVO ESTRATÉGICO 23
Tornar as informações, dados e conectividade protegidos e 100% compatível com Normativos de Segurança, incluindo a Lei Geral de Proteção de Dados.	Proteger dados, comunicações e ativos que sejam considerados estratégicos ou identifiquem pessoas físicas e jurídicas.	Aderência à LGPD.	Adequar a capacidade da tecnologia da informação aos novos desafios da transformação digital.

2.4. - Nos termos do Decreto Nº 8936, de 19 de dezembro de 2016, por não se tratar de oferta de serviços públicos digitais, consequentemente, o objeto da contratação também não será integrado à plataforma Gov.br.

2.5. - **ALINHAMENTO À ESTRATÉGIA DE GOVERNO DIGITAL**

ITEM	OBJETIVO	INICIATIVA ASSOCIADA
ITEM	Garantia da segurança das plataformas de governo digital e	Iniciativa 11.1. Garantir, no mínimo, noventa e nove por cento de disponibilidade das plataformas compartilhadas de governo digital.

11	de missão crítica	Iniciativa 11.2. Implementar controles de segurança da informação e privacidade em trinta sistemas críticos do Governo federal.

2.6. - RELAÇÃO ENTRE A NECESSIDADE DA CONTRATAÇÃO DA SOLUÇÃO DE TIC E CARACTERÍSTICAS DO OBJETO

GRUPO	ITEM	ESPECIFICAÇÃO	QTDE	JUSTIFICATIVA
ÚNICO	01	Firewall - Solução de plataforma de segurança denominada Next Generation Firewall (NGFW) com instalação, suporte, garantia e licenciamento inclusos.	04 unidades	Quantitativo referente a 02 conjuntos (clusters) que funcionará no data center do bloco D da Esplanada dos Ministérios. Eles serão o cluster principal de perímetro e o cluster interno que está substituindo 6 firewalls que existem atualmente.
	02	Solução de armazenamento de logs e relatoria, com instalação, suporte, garantia e licenciamento inclusos.	01 unidade	Quantitativo levantado de acordo com a necessidade para solução de armazenamento de logs e relatoria.
	03	Solução para gerenciamento centralizado dos equipamentos, com instalação, suporte, garantia e licenciamento inclusos.	01 unidade	Quantitativo levantado de acordo com a necessidade para o gerenciamento centralizado dos equipamentos da solução de TIC.
	04	Treinamento ministrado por profissional certificado pelo fabricante.	01 turma	01 Turma para 02 servidores públicos que atuam na coordenação de cibersegurança e privacidade.
	05	Plataforma de ZTNA - Zero Trust Network Access, com instalação, suporte, garantia e licenciamento inclusos.	01 unidade	Quantitativo levantado de acordo com a necessidade para a implantação do ZTNA no MAPA. O detalhamento da quantidade de pessoas que irão usar o serviço está descrito ao longo dos requisitos do termo de referência.

2.7. -RESULTADOS E BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

- Aumento da capacidade de resposta aos incidentes cibernéticos.
- Melhorar o acesso remoto de maneira estável aos colaboradores de forma segura.
- Aprimorar a segurança de TIC do Ministério da Agricultura e demais órgãos demandantes frente às recentes ameaças.
- Contribuir para a garantia de um nível adequado de Confidencialidade, Integridade e Disponibilidade.
- Maior visibilidade do trafego das informações e da rede, possibilitando a detecção e proteção em tempo real contra as ameaças. Com isso, será possível corrigir comportamentos inadequados; direcionar recursos para demandas mais relevantes; controlar serviços e aplicações suspeitas ou que interferem diretamente na produtividade.
- Permitir a criação de políticas de proteção da rede contra eventuais ataques de usuários mal-intencionados, através do bloqueio de portas não utilizadas e melhor controle de uso de banda de internet, com o objetivo de evitar abusos em sua utilização;
- Maior rapidez na detecção - Priorização de alertas de segurança e avisos constantes sobre normas de cibersegurança dentro de uma organização, evitando que erros humanos sejam cometidos na hora de acessar links duvidosos e outras páginas maliciosas.
- Aprimorar a detecção e bloqueio de ameaças avançadas, como malware, ataques de negação de serviço distribuídos (DDoS) e tentativas de invasão de rede.
- Melhoria na geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.

- Conseguir atender à crescente dependência dos recursos de tecnologia da informação, que fazem com que a infraestrutura de rede deva apresentar cada vez maior confiabilidade, resiliência, disponibilidade, segurança, capacidade de resolução de problemas de maneira proativa e rápida e melhorar a experiência para todos os usuários da rede do MAPA, MDA e MPA.
- Melhoria na filtragem de conteúdo web, implementando uma filtragem mais abrangente, com criação de regras de uso de aplicações web, que permitam a limitação de acesso a certas categorias de serviços, por meio de solução de armazenamento de logs e relatoria.
- Além das citadas, o NGFW permite a interação das seguintes funções em um mesmo equipamento:
    - Firewall Corporativo (Stateful Firewall).
    - Controle de aplicações (AVC-Application Visibility Control).
    - Prevenção de ameaças (IPS-Intrusion Prevention System).
    - Análises de malware "zero-day".
    - Filtro de URL e Identificação de usuários com controle granular de permissões.

3. Descrição da solução

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

3.1 . DESCRIÇÃO DA SOLUÇÃO DE TIC

3.1.1. - Trata-se de solução de proteção de rede "Next Generation Firewall", contemplando os hardwares , licenciamento, implantação, configuração, solução de armazenamento de logs e relatoria, Solução para gerenciamento centralizado dos equipamentos, treinamento, ZTNA, garantia e suporte técnico por 60 meses, de acordo com as condições, exigências, especificações e quantidades constantes deste termo de referência e seus Anexos.

3.1.2. - A solução proposta consiste em um conjunto de equipamentos e funcionalidades para proteger a rede e as aplicações do MAPA e órgãos demandantes contra ameaças cibernéticas. Essa solução de TIC oferece inspeção e filtro de tráfego interno e externo, controle de aplicação, proteção contra ameaças avançadas, IPS, proteção de DNS, ZTNA, proteção Anti-DDos na camada de aplicação, solução de armazenamento de logs e relatoria, gerenciamento dos equipamentos, entre outras funcionalidades que visam mitigar riscos de ataques e exploração de vulnerabilidades do ambiente de TI dos órgãos.

3.1.3. - A solução de TIC deverá ser constituída pelos equipamentos relacionados nos itens, sendo todos do mesmo fabricante, garantindo a entrega e execução dos serviços por uma única empresa(e sua subcontratada, se aplicável) e a total compatibilidade entre eles.

3.1.4. - A escolha do agrupamento dos itens em um único grupo visa a plena qualificação da empresa fornecedora que prestará os serviços de instalação e configuração, bem como prestará os serviços de garantia dos equipamentos, a total compatibilidade entre os mesmos, a redução de custos operacionais, a capacidade técnica de manter a solução em operação, os recursos humanos disponíveis para prestarem o devido apoio, treinamento e curva de aprendizagem e o custo total de propriedade.

3.1.5. - A descrição da solução como um todo encontrasse pormenorizada neste termo de referência, não sendo necessário, até mesmo pelo objeto da contratação, fazer a inclusão do estudo técnico preliminar, como anexo, neste termo.

3.2 . BENS E SERVIÇOS QUE COMPOEM A SOLUÇÃO DE TIC

GRUPO	ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QTDE
ÚNICO	01	Firewall - Solução de plataforma de segurança denominada Next Generation Firewall (NGFW) com instalação, suporte, garantia e licenciamento inclusos.	UNIDADE	04 unidades
	02	Solução de armazenamento de logs e relatoria, com instalação, suporte, garantia e licenciamento inclusos.	UNIDADE	01 unidade
	03	Solução para gerenciamento centralizado dos equipamentos, com instalação, suporte, garantia e licenciamento inclusos.	UNIDADE	01 unidade
	04	Treinamento ministrado por profissional certificado pelo fabricante.	CAPACITAÇÃO	01 unidade
	05	Plataforma de ZTNA - Zero Trust Network Access, com instalação, suporte, garantia e licenciamento inclusos.	SERVIÇO	01 unidade

3.3. - PARCELAMENTO DA SOLUÇÃO DE TIC

3.3.1. - O objeto do certame não será parcelado, uma vez que os bens e serviços que compõem o objeto formam um conjunto indissociável, composto pela interligação dos serviços que funcionam harmonicamente. As melhores práticas de gestão de TI se baseiam na integração dos serviços, que são indissociáveis e apresentam inter-relação entre si, de forma que assegurem o alinhamento e a coerência em termos de qualidade técnica, resultando assim, no perfeito atendimento dos princípios da celeridade, economicidade e eficiência.

3.3.2. - Somente a execução de forma integrada dos serviços garante a disponibilidade, segurança e a preservação dos dados de execução, evitando transferência de responsabilidades, nos casos de eventuais problemas causados por serviços prestados por mais de uma empresa contratada.

3.3.3. - O fornecimento de itens por meio de contratadas distintas traria enormes riscos ao projeto. Um grande risco viria da necessidade contínua de comunicação entre os diferentes fornecedores, o que, historicamente, não ocorre com fluidez nem de forma satisfatória, sendo a parte mais prejudicada, o MAPA. Além disso, há necessidade de ocorrer perfeita integração técnica entre os itens do objeto. Dessa forma, o fornecimento parcial dos itens por diferentes fornecedores traria não apenas maior complexidade, como maiores custos de integração e riscos de não execução adequada.

3.3.4. - A licitação por item poderia causar prejuízo para o conjunto da licitação (questões técnicas) ou para a economia de escala (questões econômicas), e tornaria inviável e prejudicial o bom desempenho da solução, por se tratar de serviços complementares. Ademais, por se tratar de uma solução de serviços integrados, é fundamental para a garantia da qualidade do serviço, que sejam executados por um mesmo fornecedor, dada a impossibilidade de segregação do objeto sem que haja prejuízo ao conjunto, objetivando alcançar produtividade, economicidade e eficiência na realização dos serviços.

3.3.5. - Desta forma, o agrupamento de elementos que compõem a mesma solução compõe a melhor estratégia da Administração, quando a adjudicação de itens isolados onera o "o trabalho da administração pública, sob o ponto de vista do emprego de recursos humanos e da dificuldade de controle, colocando em risco a economia de escala e a celeridade processual", vide o ACÓRDÃO Nº 5301/2013 – TCU – 2ª Câmara. É importante também, se observar o posicionamento do Egrégio Tribunal de Contas da União, nos autos do Acórdão nº 1916/2009 – Plenário, sob a matéria:

> *"15. Acerca da alegada possibilidade de fragmentação do objeto, vale notar que nos termos do art. 23, § 1º, da Lei n. 8.666/1993, exige-se o parcelamento do objeto licitado sempre que isso se mostre técnica e economicamente viável. A respeito da matéria, esta Corte de Contas já editou a Súmula n. 247 /2004, in verbis: "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes..." (grifou-se).*

3.3.6. - Depreende-se, portanto, que a divisão do objeto deverá ser implementada sempre que houver viabilidade técnica e econômica para a sua adoção.

3.3.7. - Nesse ponto, calha trazer à baila o escólio de Marçal Justen Filho: "O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. Não é possível desnaturar um certo objeto, fragmentando-o em contratações diversas e que importam o risco de impossibilidade de execução satisfatória." (Comentários à Lei de Licitações e Contratos Administrativos. 10. ed. São Paulo: Dialética, 2004. p. 209)."

3.3.8. - Adicionalmente, em virtude da especificidade do objeto, pode-se afirmar ser tecnicamente inadequado o seu desmembramento, sob pena de não se atender o objetivo buscado, no sentido de fortalecer a disponibilidade, segurança, a preservação dos dados e ativos de TI do MAPA na manutenção da operabilidade do ambiente de TI.

3.3.9. - Ainda, sob o ponto de vista econômico, não há elementos nos autos que permitam concluir que a adoção do parcelamento do objeto, seria, no caso concreto, mais vantajosa para o MAPA.

3.3.10. - Por fim, o objeto não será parcelado, pois constitui-se em uma única solução de TIC e os serviços que compõem o objeto licitado são serviços de mesma natureza, dependentes entre si, e sua divisão impactaria na execução do projeto e tornaria a contratação menos econômica, eficaz e eficiente para a Administração. Assim, considerando-se a inviabilidade técnica e econômica para o parcelamento do objeto da presente contratação, bem como consideradas as suas respectivas peculiaridades, interdependência e natureza acessória entre os serviços que compõem o objeto, a contratação pretendida deverá ser realizada em um único grupo.

4. Requisitos da contratação

4.1. REQUISITOS DE NEGÓCIO

- Aquisição de solução de segurança de perímetro contemplando o hardware, software, licenciamento, instalação, configuração, treinamento, garantia, atualizações e suporte técnico, em atendimento à solicitação (Documento de oficialização de demanda SEI Nº 27476908 da Coordenação-Geral de Infraestrutura, Cibersegurança e Serviços da Subsecretaria de Tecnologia da Informação do MAPA.

- Deverá fazer parte da composição da solução a elaboração de projeto de instalação e configuração de modo a possibilitar a análise prévia da equipe técnica do MAPA quanto aos procedimentos necessários para a implementação da solução, com o planejamento de janelas de indisponibilidades e plano de comunicação de modo a dar maior transparência do processo para os usuários da rede MAPA/MDA/MPA.
- Todos os serviços de instalação e configuração deverão ser executados pela contratada, devendo ser acompanhadas por servidores do MAPA.
- Melhorar e garantir o perfeito funcionamento da infraestrutura de rede do Ministério da Agricultura e Pecuária(MAPA) e seus Ministérios demandantes através da modernização da arquitetura de firewall do Ministério, provendo equipamentos mais confiáveis e robustos.
- Prover e Garantir a segurança das informações como também a continuidade dos serviços de TIC.
- Assegurar a confidencialidade, disponibilidade e integridades das informações do MAPA e seus Ministérios demandantes em conformidade com a LGPD.
- Melhorar a identificação e o rastreamento das tentativas de invasão às redes.
- Melhorar a proteção da infraestrutura de TIC de modo a impedir que a rede seja utilizada para outros fins (por exemplo: Mineração de bitcoins, links de internet utilizados para download de conteúdo ilícito , ataques de negação de serviço-DOS, entre outros). Melhoria no reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos. Melhorar o tempo de resposta aos ataques com automação de segurança.
- A solução deverá ter ainda em sua composição um item para treinamento, para garantir que ocorra a transferência do conhecimento para os servidores e colaboradores que atuam na infraestrutura de TI do MAPA.
- De modo a tornar viável o investimento sem riscos da continuidade dos serviços e com garantia de atualização de softwares e componentes da solução, será exigido garantia e suporte técnico por período não inferior a 60 meses.
- A solução também deverá incluir a tecnologia ZTNA.
- Atender prontamente ao aumento de novos serviços on-line.

4.2. REQUISITOS LEGAIS

A presente contratação sujeita-se à legislação pertinente, mormente aos diplomas a seguir elencados, bem como às demais normas gerais que se apliquem, considerando-se a legislação consolidada com as respectivas alterações subsequentes:

4.2.1 . LEIS

- Lei Nº 14.133, de 1º de Abril de 2021.
- Lei Nº 13.709, de 14 de Agosto de 2018 e Lei Nº 13.853, de 08 de julho de 2019. (LGPD).
- Decreto-Lei Nº 200, de 25 de fevereiro de 1967 - dispõe sobre a organização da Administração Federal, estabelece
- diretrizes para a Reforma Administrativa.

4.2.2 . DECRETOS

- Decreto Nº 9.507/2018: Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;
- Decreto Nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;
- Decreto-Lei Nº 200, de 25 de fevereiro de 1967 - dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa.
- Decreto Nº10.947, de 25 de Janeiro de 2022. (Regulamenta o inciso VII do caput do art. 12 da Lei nº 14.133, de 1ºde abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional.)
- Decreto Nº 10.569, de 09 de dezembro de 2020 - Estratégia nacional de Segurança da Infraestrutura Críticas.

4.2.3 . INSTRUÇÕES NORMATIVAS

- Instrução Normativa SGD/ME Nº 94, de 23 de Dezembro de 2022 (Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal).
- Instrução Normativa Nº 5 de 25 de maio de 2017 (Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.)
- Instrução Normativa SEGES/ME Nº 65, de 7 de Julho de 2021-Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

- Boas práticas, orientações e vedações para contratação de Ativos de TIC - Versão 4. Orientações específicas para a aquisição de Ativos de TIC. (Este guia está vinculado à Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, conforme § 2º do Art. 8º)
- Instruções normativas SEGES Nº 58, de 08 de agosto de 2022 - Dispõe sobre a elaboração de estudo técnicos preliminares-ETP para a aquisição de bens e contratação de serviços e obras, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o ETP Digital.
- Instrução normativa Nº 01 , de 19 de janeiro de 2010. - Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal, autárquica e fundacional e dá outras providências.)
- Instrução Normativas SEGES/ME Nº 81, de 25 de Novembro de 2022, a qual Dispõe sobre a elaboração do Termo de Referência – TR, para a aquisição de bens e a contratação de serviços, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema TR digital.

4.2.4 . PORTARIAS

- Portaria MGI Nº 43, de 31 de Janeiro de 2023. (Disciplina o compartilhamento de atividades de administração patrimonial, de material, de gestão de pessoas, de serviços gerais, de orçamento e finanças, de contabilidade, de logística, de contratos, de tecnologia da informação, de planejamento governamental e gestão estratégica e de outras atividades de suporte administrativo realizadas por meio de arranjos colaborativos entre Ministérios ou modelos centralizados, e dispõe sobre medidas transitórias decorrentes da edição da Medida Provisória nº 1.154, de 1º de janeiro de 2023.)
- Portaria GSI/PR Nº 120, de 21 de Dezembro de 2022. (Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal).
- Portaria MAPA Nº 136, de 25 de Maio de 2021 (Aprova a Política de Segurança da Informação do Ministério da Agricultura, Pecuária e Abastecimento - POSIC/MAPA.)
- Portaria MAPA Nº 499, de 17 de Outubro de 2022 - Política de Gestão de Vulnerabilidades Cibernéticas.
- Portaria GSI/PR Nº 93, de 18 de outubro de 2021 - Aprova o glossário de segurança da informação.

4.3. REQUISITOS TEMPORAIS

- O serviço de substituição de hardware será prestado na modalidade 24x7x365, ou seja, estará disponível para acionamento 24 horas por dia, 7 dias por semana, devendo substituir quaisquer peças ou componentes defeituosos em um prazo máximo conforme último tópico estipulado no item 7.8.2, contados a partir da data de abertura do chamado (ticket de atendimento).
- O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da Contratada, devidamente aceita pelo fiscal técnico do contrato.
- A entrega total , configuração e implantação completa de todos os bens e da solução de TIC deve ocorrer em no máximo 60 dias úteis a partir da assinatura da ordem de serviço, devendo ser agendada com antecedência mínima de 48 horas.
- Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local seguro para download dos arquivos de instalação.
- A contratada deverá cumprir todos os prazos descritos neste estudo técnico preliminar, respeitando os prazos máximos estabelecidos. A seguir, segue um resumo de alguns requisitos temporais mais importantes:

ID	DESCRIÇÃO	PRAZO MÁXIMO(DIAS ÚTEIS)
01	Assinatura do contrato.(MAPA e Contratada)	Início dos prazos
02	Realização da reunião inicial. (MAPA e contratada). Apresentação formal da equipe de fiscalização do contrato e do preposto. (contratante e contratada) Repasse à contratada de conhecimentos necessários à execução dos serviços (contratante); Entrega do termo de compromisso e de ciência devidamente assinados (contratada).	05 dias úteis após o ID 1.
03	Entrega do projeto da implantação (Contratada).	5 dias úteis após o ID 2.
04	Análise e aprovação do projeto de implantação (contratante).	5 dias úteis após o ID 3.
05	Finalização da execução dos serviços e instalação dos bens. (Contratada)	60 dias úteis após o ID 4.
06	Início do treinamento	10 dias após o ID 5 ou a depender da disponibilidade de horário/data dos recursos do

		MAPA.

4.4. REQUISITOS CULTURAIS, SUSTENTABILIDADE E SOCIAIS

4.4.1. REQUISITOS CULTURAIS

- Durante a execução de tarefas no ambiente do MAPA, os funcionários da empresa contratada deverão observar, no trato c om os servidores públicos em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público.
- A documentação e os manuais de operação da solução deverão ser apresentados preferencialmente no idioma Português (Brasil – PT-BR) e, em sua ausência, deverão ser apresentados em idioma Inglês. Ademais, deverá entregar os documentos solicitados na forma digital, com vistas a evitar ou reduzir o uso de papel e impressão, em atendimento ao Art. 9º da Política de Nacional de Resíduos Sólidos (Lei nº 12.305, de 2 de agosto de 2010).
- A abertura de chamados técnicos e encaminhamento de demandas deverão ser realizados, obrigatoriamente, sob a forma eletrônica, evitando a impressão de papel. Além disso, as configurações de hardware e softwares deverão ser realizadas visando alto desempenho com a utilização racional de energia.

4.4.2. REQUISITOS DE SUSTENTABILIDADE AMBIENTAL

Em conformidade com o Guia nacional de Contratações Sustentáveis (https://www.gov.br/agu/pt-br/composicao/cgu/cgu/guias /guia-de-contratacoes-sustentaveis-set-2023.pdf) , a contratada deverá cumprir com os seguintes requisitos de sustentabilidade ambiental:

- Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantia máxima proteção durante o transporte e o armazenamento.
- Somente poderão ser utilizados na execução dos serviços, equipamentos que possuam a certificação de que trata a portaria Inmetro Nº 170, de 2012 **ou** que possuam comprovada segurança, compatibilidade eletromagnética e eficiência energética equivalente.
- Só será admitida a oferta de equipamentos que **não** contenham substâncias perigosas em concentração na diretiva RoHS (Restriction of Certain Hazardous Substances) tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio(Cd), Bifenil polibromados(PBBs) e éteres difenilpolibromados(PBDEs).

A comprovação do disposto neste artigo poderá ser feita mediante apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, **ou** por qualquer outro meio de prova que ateste que o bem fornecido cumpre com as exigências do edital.

4.4.3. REQUISITOS SOCIAIS

Quanto aos critérios sociais, todos os profissionais da Contratada que desempenharão as atividades em contato direto com a Contratante deverão cumprir os seguintes requisitos:

- Estar vestidos de forma adequada ao ambiente de trabalho físico ou virtual, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da Contratante ou que ofenda o senso comum de moral e bons costumes;
- Respeitar todos os servidores, funcionários e colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo;
- Atuar dentro das instalações do MAPA e órgãos demandantes com urbanidade e cortesia.

4.5. REQUISITOS DE VISTORIA TÉCNICA

- A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09:00 às 12:00 / 14:00 às 17:00 horas.
- Embora opcional, é recomendável a realização de visita técnica, e esta deve ser realizada até 03 (três) dias antes da data fixada para a sessão pública, mediante agendamento prévio de acordo com os contatos da Subsecretaria de Tecnologia da Informação do MAPA através dos e-mails: coseg@agro.gov.br e/ou cginfra.sti@agro.gov.br. (Telefone 3218-2208).
- A realização da visita técnica não se consubstancia em condição para a participação na licitação, ficando, contudo, as licitantes cientes de que após a apresentação das propostas não serão admitidas, em hipótese alguma, alegações no sentido da inviabilidade de cumprir com as obrigações, em face do desconhecimento dos serviços e de dificuldades técnicas não previstas.
- Para vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprando sua habilitação para a realização da vistoria.

- O MAPA emitirá "Declaração de Realização de Vistoria Técnica", ao qual deverá ser apresentado junto a proposta de preços, conforme Anexo-Vistoria, deste Termo de Referência para os licitantes que fizerem a vistoria. Caso o licitante não tenha realizado a vistoria, deverá prestar declaração formal assinada, também conforme anexo-vistoria.
- A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

Abaixo, seguem os requisitos tecnológicos:

4.6 . REQUISITOS TÉCNICOS GERAIS DA SOLUÇÃO DE TIC

- A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado.
- Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior data da proposta.
- Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.
- A solução de balanceamento deverá ser fornecida em Alta Disponibilidade do tipo Ativo/Ativo.
- Transferir todas as regras e configurações dos Firewalls em produção atualmente.
- Tanto os dispositivos físicos (“appliance”) quanto seus softwares deverão ser novos, de primeiro uso, e disponibilizados em suas versões mais atualizadas.
- Os equipamentos dos itens 01, 02, 03 e 05 devem ser do mesmo fabricante, completamente interoperáveis, e devem ser capazes de fazer escalonamento de desempenho com movimentação de appliances dentro da topologia da rede.
- Autenticação de dois fatores, no que couber, principalmente na plataforma de gerenciamento (item 3 da contratação).
- A solução deverá possuir a quantidade de transceptores suficientes para conectar toda a solução à rede corporativa, o que inclui a gerência.

4.6.1. REQUISITOS GERAIS DO ITEM 01

- Solução integrada de proteção de rede do tipo “Next Generation Firewall” (NGFW), formada pelo conjunto de dispositivos ,obrigatoriamente físicos (appliances), interconectados e operando em modo de alta disponibilidade, com recursos de virtualização de sistemas, filtragem de pacotes, filtro de URL (web-filtering) com controle de transmissão de dados e de acesso à internet, controle de aplicação, controle por meio de identificação de usuários, controle de uso de largura debanda (QoS), VLAN, NAT, VPN, DHCP services (server, client e relay), sistema de prevenção de intrusão (IPS) e prevenção contra ameaças de vírus, spywares e malwares, incluindo os de tipo “Zero Day”.
- Conjunto de dispositivo físico (appliance) de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), sistema operacional embarcado no dispositivo e software para sua gestão e monitoramento, permitindo o controle granular das políticas de segurança de rede, atuando além da camada 2 a 4 do modelo OSI, ou seja, além da filtragem por endereços MAC e endereços e portas TCP/IP, permitindo a configuração de políticas de segurança também por aplicações, incluindo seu conteúdo, usuários e tipos de tráfego de rede, recursos tipicamente executados em camada 7.
- O Firewall NGFW deve ser do tipo “rackmount”, permitindo sua instalação em racks de Datacenter , devendo consumir um espaço no rack de no máximo 4U por dispositivo.
- Não serão aceitos equipamentos servidores (“rack servers”) e sistemas operacionais de uso genérico, como Microsoft Windows ou distribuições Linux para usuários finais, adaptados para funcionar como “appliance” físico, ou seja, a solução como um todo de ser fabricada pelo mesmo fornecedor, tanto em seus componentes físicos de hardware quando seus softwares embarcados principais, sendo vedada solução de software livre.
- Todas as funcionalidades da solução Firewall NGFW deverão operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo após o fim do contrato, e mesmo que o MAPA não tenha mais o direito de receber atualizações por descontinuidade da solução por parte da fabricante.
- Os appliances devem permitir aceso ao equipamento via interface de comando(CLI), console, SSH, além de interface web HTTPS.
- O serviço de VPN disponibilizado pela solução de firewall atual deve ser migrado e colocado em funcionamento na nova solução de ZTNA contratada, sob total responsabilidade da contratada, permitindo que todos os acessos e regras existentes continuem em pleno funcionamento.
- Os appliances deverão vir acompanhados de todos os conectores, cabeamento e peças de fixação no Rack, necessários à sua instalação e funcionamento, conforme as especificações deste Termo de Referência.
- Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário.
- As soluções a serem fornecidas deverão estar totalmente licenciada para as funcionalidades mínimas listadas a seguir: Controle por política de firewall, controle de aplicações, prevenção de ameaças, Filtro de URL, Prevenção de ameaças avançadas (Zero Day), Identificação de usuários, QoS, VPN site-to-site (IPsec), VPN client-to-side e DNS Security.

4.6.1.1. - ACESSÓRIOS

- Além dos cabos de alimentação de energia, o equipamento deve ser acompanhado também dos seguintes acessórios obrigatórios:
    - Trilhos deslizantes e demais itens necessários para instalação em rack padrão 19 polegadas.
    - Cabos fibre channel com conectores LC/LC com no mínimo 5 (cinco) metros de comprimento, na mesma quantidade de transceivers ofertados na solução.
    - Cabos e interfaces de interconexão entre os appliances físicos para configuração da solução em modo de "alta disponibilidade", considerando-se que os firewalls NGFW ficarão próximos um do outro na rack, com distância entre eles de até 02 (dois) U.
    - Todos os drivers, softwares e licenças necessários para o perfeito funcionamento de todos os componentes da solução.
    - Documentação com a especificação técnica dos equipamentos.
    - Manuais de instalação, operação e gerenciamento.
    - Todos os documentos e manuais deverão ser confeccionados preferencialmente em língua portuguesa e fornecidos no momento da entrega do equipamento por meio de mídia física ou digital.

4.6.1.2 - Requisitos Específicos do Item 01

As quatro unidades devem operar em cluster (02 clusters separados) e ter as seguintes capacidades/características:

- Deve suportar operação em cluster ativo-ativo sem a necessidade de licenças adicionais.
- Deve possuir throughput de, pelo menos, 14 Gbps de Threat Protection ou nome equivalente, considerando no mínimo as funcionalidades de firewall, IPS, controle de aplicação e proteção de malware ativadas.
- Deve possuir throughput de, pelo menos, 18 Gbps de Next Generation firewall, considerando no mínimo as funcionalidades de firewall, IPS e controle de aplicação habilitadas.
- Deve possuir , no mínimo, 23 Gbps de IPS throughput.
- Deve possuir , no mínimo, 23,8 de Firewall Throughput.

Deve suportar no mínimo:

- 3.000.000 (três milhões) de conexões simultâneas.
- 230.000 (Duzentos e trinta mil) novas conexões por segundo.
- 08 interfaces físicas de rede do tipo GE RJ 45.
- 08 interfaces físicas de rede do tipo GE SFP.
- 12 interfaces físicas de rede do tipo 10 GE SFP 28.
- 02 interfaces físicas de rede do tipo 40 Gbps QSFP+ ou superior.
- 01 interface física de rede de 1Gbps dedicada para gerenciamento.
- Homologação da Agência Nacional de Telecomunicações (ANATEL), exigência a ser comprovada por meio da apresentação do certificado quando da entrega dos documentos de habilitação.
- Possuir disco do tipo Solid State Drive(SSD) de, no mínimo, 480 Gb para armazenamento do sistema operacional e registro de logs.
- O Throughput e as interfaces solicitadas neste item deverão ser comprovados através de datasheet públicos na internet.
- Não serão aceitas declarações de fabricantes informando números de performance e interfaces.
- Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers /transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização.
- Suporte a RFC 4291 de Arquitetura de endereçamento IPv6.
- Deve suportar Dual stack ipv4/ipv6 e NAT64.
- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
- Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP v4 e v6 sem duplicação da base de objetos e regras.

4.6.2. REQUISITOS DE SUPORTE/GARANTIA E MANUTENÇÃO

4.6.2.1 - GARANTIA

- Nos processos de aquisições de bens de Tecnologia da Informação - TI, devido às suas características técnicas e por serem investi mentos de alto custo, será sempre necessário que esses bens sejam acompanhados de uma garantia e de suporte para fins de assegurar o perfeito funcionamento da solução, como previsto no documento Boas Práticas, Orientações e Veações para contratação de ativos de TIC – Versão 4 , vinculado à Portaria nº 20 de 14 de julho de 2016 da Secretaria de Tecnologia da informação do Ministério do Planejamento – Portaria MP /STI nº 20/2016 – e ratificado pela Instrução Normativa nº1, de 4 de abril de 2019. Esse documento, "Orientações para elaboração/ajuste de especificações técnicas de ativos de TI – Versão 4.0", orienta como especificar nas contratações de bens de TI da

Administração Pública Federal – APF, padronizando, qual o tempo de vida útil de cada conjunto de ativos de TI e o referido tempo de garantia. No item 1.2 - Aquisição de Ativos de TI com garantia versus contratação de serviços de manutenção, temos os seguintes subitens que devem ser observados:

"1.2.1 Os ativos de TI devem ser adquiridos com garanti a de funcionamento provida pelo fornecedor durante sua vida útil, salvo quando justificado o contrário e com relação ao ativo em específico.
1.2.2 Tal procedimento se justifica pelo fato de que, de forma geral a contratação, a posteriori, de serviços de manutenção para ativos fora de garanti a, usualmente é mais onerosa para a Administração do que quando o bem é adquirido com garanti a para toda sua vida útil. Ainda, os contratos de manutenção têm seus custos elevados na medida em que os bens manutenidos se tornam obsoletos. Ou seja, quanto mais antigo for o ativo de TI, menor seu valor comercial e maior será seu custo de manutenção, devido à dificuldade de provimento de peças de reposição e do maior risco do fornecedor descumprir os níveis de serviço exigidos para reparo desses equipamentos.
1.2.3 Tem-se, portanto, que um dos fatores que para definição do posicionamento adequado da tecnologia (item 1.1) é o tempo de vida útil previsto para utilização do ativo e, por conseguinte, o tempo de garanti a de funcionamento a ser contratado." (GRIFO NOSSO)

- No item 1.4 - Orientações Específicas Sobre o Ciclo de Vida, é definida a padronização do ciclo de vida de cada ativo de TI, fazendo com que a Administração Pública federal especifique da mesma forma as aquisições de bens de TI. A definição do subitem 1.4.5 estabelece a vida útil dos Ativos de Rede, tais como: servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros:

  "1.4.5.1 Para aquisição de servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros, deve-se considerar o tempo de vida útil mínimo de 5 (cinco) anos para fins de posicionamento da tecnologia e de garantia de funcionamento." (GRIFO NOSSO)

- Ressalta-se que os equipamentos a serem adquiridos nessa contratação, firewalls de próxima geração, solução de armazenamento de logs e relatoria e solução de gerenciamento centralizado, são equipamentos de rede, de segurança e de aplicação, e, portanto, considera-se o tempo de vida útil desses equipamentos de, no mínimo, 5 anos (60 meses).
- Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos e demais licenças/firmwares/softwares fornecidos com o objetivo de obter novas funcionalidades e correção de bugs. Durante o prazo de garantia, deve ser possível realizar a atualização das assinaturas de proteção da solução.
- Os chamados poderão ser abertos diretamente com a contratada, autorizada oficial do fabricante ou com o próprio fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7x365 (24 horas por dia, 7 dias por semana);
- A contratada deve fornecer garantia de reposição de hardware, pelo prazo de vigência do contrato, para situações que sejam identificados problemas constantes na solução fornecida.
- A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se necessário, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.
- Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas). Ao final do contrato, o MAPA deve ter as licenças mais recentes instaladas em modo definitivo (licenças perpétuas). Isso é necessário para garantir que ao término do contrato, entre o fim do mesmo e uma nova contratação, nenhuma das ferramentas contratadas deixe de funcionar por falta de licença de software.
- Entendemos que as assinaturas de malware, IPS/IDS e atualizações do software serão interrompidas ao fim do contrato, mas as ferramentas têm que seguir funcionando em suas versões mais recentes na data de finalização do contrato.
- O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada.
- Os serviços de "Garantia" também incluem:
  - Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas de fabricação, desenvolvimento ou ocasionada pelo uso normal dos equipamentos.
  - Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros.
  - Esclarecimento de dúvidas de alto nível.
  - Instalação de novas versões ou atualizações e patches.

4.6.2.2 - DEFINIÇÃO E DISCRIMINIÇÃO DOS ITENS DE GARANTIA/SUPORTE/MANUTENÇÃO

- Neste sentido, observa-se que no mercado a garantia pode ser adquirida de forma embuti da no valor total do bem ou pode ser separada em um item exclusivo; isso ocorre, por exemplo, quando necessita-se da valoração de cada componente da solução, neste caso da garantia. Em ambos os casos, a garantia é item indissociável do bem; logo, sua contraprestação é na sua entrega, ocasionando a necessidade da justa liquidação financeira em conformidade com o subitem 1.2.1. das Boas práticas, orientações e vedações para contratação de ativos de TIC – Versão 4 (https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes_ativos-de-tic-v-4.pdf) e pelo Art. 50, parágrafo único da Lei 8.078 /1990.

> *"Art. 50. A garanti a contratual é complementar à legal e será conferida mediante termo escrito. Parágrafo único. O termo de garantia ou equivalente deve ser padronizado e esclarecer, de maneira adequada em que consiste a mesma garantia, bem como a forma, o prazo e o lugar em que pode ser exercitada e os ônus a cargo do consumidor, devendo ser-lhe entregue, devidamente preenchido pelo fornecedor, no ato do fornecimento, acompanhado de manual de instrução, desinstalação e uso do produto em linguagem didática, com ilustrações." Lei nº 8.078/1990 (GRIFO NOSSO)*

4.6.2.3 - PAGAMENTO DA GARANTIA/SUPORTE/MANUTENÇÃO

- O artigo 40,inciso I, da Lei 14.133/2021, estabelece que as compras públicas sempre que possível devem pautar-se pelas condições de aquisição e pagamento do setor privado, confirmado pelo Acórdão 1177/2014 – Plenário, sendo juridicamente viável aquisição de bens de informática, com a prestação de garantia por determinado período, mediante pagamento integral no momento da entrega e aceitação dos equipamentos.

> *Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:*
> *I - condições de aquisição e pagamento semelhantes às do setor privado;*
> *e "Jurisprudência - Número 196*
> *É juridicamente viável a aquisição de bens de informática, com a prestação de garantia por determinado período, mediante o pagamento integral no momento da entrega e aceitação dos equipamentos. Consulta apresentada pelo Presidente do Tribunal Superior do Trabalho indagou ao Tribunal a possibilidade de aquisição de bens de informática, com a prestação de garantia (assistência técnica de preços e serviços) por determinado período, mediante o pagamento*
> *integral do valor contratado no momento da entrega e aceitação dos equipamentos. O relator, de início, mencionou que o objeto da Consulta não trata de pagamento antecipado "típico", em que a entrega do numerário ao fornecedor é feita antes do recebimento do bem ou serviço pela Administração. Na espécie, trata-se de contratação de equipamentos de informática, em que está embutida a prestação de um serviço (assistência técnica durante o período de garanti a), distinção que, na ótica do relator, tem relevância, pois no pagamento antecipado o risco para a Administração configura-se bem maior, já que efetuado antes de qualquer contraprestação por parte do fornecedor. Na situação em tese, o pagamento só seria realizado após o recebimento do bem, objeto principal da contratação. A prestação futura se referia apenas ao serviço de suporte técnico durante o período de garanti a, espécie de acessório em relação ao objeto principal. Depois de estabelecer tal distinção, o relator concluiu que é possível a contratação de bens de informática, com a prestação de garantia, realizando-se o pagamento integral do valor contratado quando do recebimento dos bens." (GRIFO NOSSO)*

- O pagamento antecipado da garantia no momento da entrega e aceitação dos equipamentos é, em tese, considerado, por vezes em diversos órgãos da APF uma prática comum e aceitável. Entende-se que isto se dê pela mitigação de riscos inerentes a variações econômicas, crises e volatilidades, enfrentados em um cenário de 5 (cinco) anos de prestação de serviço.
- Esse entendimento é explicitado no Acórdão TCU 2569/2018 que tratou da auditoria operacional, práticas comerciais adotadas por grandes fabricantes de tecnologia da informação (TI) na relação com a administração pública, por ocasião da contratação de licenciamento de software e seus serviços agregados, em que os serviços agregados são normalmente comercializados junto com as licenças na primeira aquisição, quando têm a conotação de "garantia", remetendo-se ao Código de Defesa do Consumidor, sendo a renovação opcional após o fim da vigência do primeiro período contratado. Nesse contexto, costuma-se, inclusive, exigir o pagamento à vista:

> *"156. Os fabricantes costumam exigir o pagamento à vista para o fornecimento de licenças e de serviços agregados, o que pode resultar na não utilização dos itens adquiridos devido à demora para viabilizar a utilização do software ou à interrupção de projetos. Por outro lado, o pagamento parcelado costuma incluir um custo financeiro da operação no preço final obtido pelas organizações públicas." (GRIFO NOSSO)*
> *"157. Os grandes fabricantes de soluções de TI costumam adotar, no país e também no exterior, a venda de licenças e de serviços agregados mediante recebimento de quantia à vista, seja quando a venda é direta, seja por intermédio de um representante (peça 69, p. 4, questão 6.b; peça 92, p. 4, questões 6.2 e 6.3; peça 95, p. 3,questão 6.2; peça 100, p. 2). Tanto as licenças quanto os*

> *serviços agregados possuem peculiaridades que devem ser consideradas pelos gestores na decisão de optar-se pelo pagamento à vista ou parcelado durante o processo da contratação. Além disso, a compra de licenças e de serviços agregados deve ocorrer em momento*
> *oportuno dos projetos para evitar que haja dispêndio de recursos em período no qual não há utilização desses itens." (GRIFO NOSSO) "172. O modelo de pagamento à vista é adotado pela maioria dos fabricantes tanto para licenças como para serviços agregados (parágrafo 157)." (GRIFO NOSSO)*

- Além disso, também acredita-se estar presentes as justificativas para comprovar a situação de excepcionalidade da antecipação de pagamento em observância ao Acórdão TCU 2569/2018 e a ON AGU nº 37/2011:

> *Acórdão TCU 2569/2018 "165. Apesar de o arcabouço legal supramencionado induzir à percepção de inviabilidade de pagamento à vista pela prestação de serviços, este Tribunal já demonstrou o entendimento de que o pagamento antecipado é admiti do em situações excepcionais (Acórdãos 1.341/2010, de relatoria do Ministro-Substituto Marcos Bem querer; e 1.160/2016, de relatoria do Ministro Augusto Nardes, todos do Plenário do TCU), ocasiões em que a APF deve demonstrar o interesse público em se adotar tal prática, bem como obedecer aos seguintes critérios: (i) que o pagamento antecipado represente condição sem a qual não seja possível obter o bem ou assegurar a prestação do serviço, ou propicie sensível economia de recursos, (ii) existência de previsão no edital de licitação ou nos instrumentos formais de contratação direta e, (iii) adoção de indispensáveis cautelas ou garanti as." (GRIFO NOSSO)*
> *ON AGU nº 37/2011 "A antecipação de pagamento somente deve ser admiti da em situações excepcionais, devidamente justificada pela administração, demonstrando-se a existência de interesse público, observados os seguintes critérios: 1) represente condição sem a qual não seja possível obter o bem ou assegurar a prestação do serviço, ou propicie sensível economia de recursos; 2) existência de previsão no edital de licitação ou nos instrumentos formais de contratação direta; e3) adoção de indispensáveis garanti as, como as do art. 56 da lei nº 8.666/93, ou cautelas, como por exemplo a previsão de devolução do valor antecipado caso não executado o objeto, a comprovação de execução de parte ou etapa do objeto e a emissão de título de crédito pelo contratado, entre outras." (GRIFO NOSSO)*

- Ante ao exposto, ratifica-se o posicionamento pelo pagamento à vista dos 5 (cinco) anos - 60 meses - de prestação de serviços agregados de garantia e suporte, assim como da solução de TIC como um todo.

4.6.3. MANUTENÇÃO

- Em caso de falha do(s) hardware(s), caso não seja feita a troca conforme prazo especificado, a contratada deve disponibilizar hardware(s) reserva(s) que irá(ão) permanecer em ambiente de produção do MAPA até o retorno do (s) hardware(s) original(is) reparado ou novo em substituição, a critério do MAPA e órgãos demandantes (MPA e MDA).
- Deverá assegurar que o hardware substituto, em qualquer caso, seja igual ao contratado inicialmente ou que possua características superiores a este, desde que estejam homologadas pelo fabricante como parte compatível da solução. As peças de substituição devem ser novas, não sendo aceitas peças usadas ou recondicionadas;
- A substituição do hardware será considerada consumada no momento em que a solução voltar ao seu funcionamento normal e for aceita formalmente pela equipe técnica do MAPA.

4.6.3.1. MANUTENÇÃO PREVENTIVA

- A manutenção preventiva será destinada a atualizar os componentes do software e a realizar quaisquer operações que evitem uma parada parcial ou total da solução.
- Durante a manutenção preventiva, a contratada deverá analisar toda a solução, sua condição atual de funcionamento, seus logs de sistemas e sugerir mudanças para uma melhor utilização e retornos dos equipamentos/ferramentas associadas à solução de TIC. A equipe técnica do MAPA junto ao fiscal técnico decidirá sobre a aplicação ou não das recomendações.
- A manutenção preventiva deverá ser executada, obrigatoriamente 01 vez por mês, conforme cronograma a ser definido entre o fiscal técnico e equipe técnica da contratada. O cronograma anual poderá sofrer adequações durante o ano vigente , desde que a contratada e o MAPA estejam de acordo e que não seja descumprido o atendimento mensal. Se a fiscalização técnica do contrato justificar que a manutenção preventiva não está sendo suficiente, o MAPA poderá solicitar a alteração para, no máximo, 02 visitas preventivas mensais.
- Deverá ser gerado um relatório mensal contendo todas as evidências das visitas técnicas preventivas sem necessidade de solicitação por parte da fiscalização contratual.

4.6.3.2. MANUTENÇÃO CORRETIVA

- A manutenção corretiva será destinada a resolver os defeitos apresentados pelos componentes de software e hardware de toda solução de TIC do contrato, compreendendo também a atualização de versões e correções dos componentes

de software e hardware que se fizerem necessários. Ademais, 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.

- A manutenção corretiva será realizada sempre que a solução apresentar falha que impeça o seu funcionamento regular e necessite de uma intervenção técnica especializada e, caso necessário, a substituição dos componentes. A manutenção corretiva pode ser solicitada a qualquer momento em que o sistema apresente pane, deficiência ou dificuldade de operação.
- As visitas para prestação dos serviços de manutenção preventiva e corretiva, independente da quantidade necessária, não deve implicar em custos adicionais para o MAPA.
- Entende-se por "manutenção corretiva", toda atividade do tipo corretiva não periódica que variavelmente poderá ocorrer durante o período de garantia. A atividade corretiva possui suas causas em falhas e erros no software/hardware e trata da correção dos problemas atuais e não iminentes de fabricação dos equipamentos. Essa "garantia" inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:
    - Do hardware: Desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação ou ocasionada pelo uso normal dos equipamentos, atualização da versão de drivers e firmwares, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados.
    - Do Software: Desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, outros problemas envolvidos, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados. Quanto às atualizações pertinentes aos softwares, entende-se como atualização o provimento de toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas releases, versions, builds, upgrades, englobando inclusive versões não sucessivas, nos casos em que a solicitação de atualização de tais versões ocorra durante o período de garantia.
- A contratada deverá substituir as peças quebradas, com defeito ou gastas pelo uso normal dos equipamentos, por outras de configuração igual ou superior, originais e novas, sem que isso implique acréscimo aos preços contratados. Substituir, temporária ou definitivamente, o equipamento defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas, novo e de primeiro uso, quando então, a partir de seu efetivo funcionamento, ficará suspensa a contagem do prazo de reparo, nos casos em que não seja possível o reparo dentro dos prazos máximos estipulados.
- A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pelo Contratante, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato. O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software. Deverá fornecer, ainda, serviços de configuração, instalação, transferência de conhecimento, com licenciamento e garantia durante o período contratual, ao longo do qual deverão ser fornecidas sem custo adicional todas as correções (patches) e atualizações, inclusive de “firmware”, da solução, sempre que houver adição de novas funcionalidades ou correções.
- A contratada deverá substituir os appliances físicos e componentes e/ou acessórios que apresentem defeitos, de forma definitiva, e qualquer outro equipamento físico fornecido na contratação como um todo, após a intervenção corretiva nos seguintes prazos:
    - Máximo de 15 dias úteis para os equipamentos do item 01.
    - Máximo de 20 dias úteis para os demais componentes e acessórios.

4.7. REQUISITOS DE PROJETO, IMPLEMENTAÇÃO E INSTALAÇÃO

A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:

- Reunião de alinhamento para criação do escopo do projeto previamente a instalação.
- Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte do MAPA. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo e ativo/ativo), a ser decidido no momento da instalação.
- Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados.
- Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos.
- Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7.
- Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução.
- Configuração de todos os componentes necessários à perfeita execução de todos os itens da contratação de acordo com as exigências levantadas.

- Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças.
- Todos os cabos de conexão, acessórios e itens relacionados ao completo funcionamento das soluções adquiridas devem ser fornecidos pela contratada.

4.8. REQUISITOS GERAIS DO ITEM 02 (Appliance Físico)

- Deverá estar devidamente licenciada para:
  - Suportar a coleta de, no mínimo, 25 GB de logs diários.
  - Espaço de armazenamento de, no mínimo, 12 TB.
- Deve suportar:
  - Pelo menos duas interfaces 10GE.
  - Suportar a configuração de RAID 0, 1, 5, 10, para os discos internos. Possuir fonte de alimentação interna, redundante e hot-swap.
  - Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de endof- life e end-of-sale.
- Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.
- Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.
- Suporte a geração de relatórios de tráfego em tempo real. Deve ser possível ver a quantidade de logs enviados de cada
- dispositivo monitorado. Deve possuir mecanismos de remoção automática para logs antigos.
- Permitir importação e exportação de relatórios, pelo menos, no formato CSV.
- Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV.
- Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.
- Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.
- A solução deve ter relatórios predefinidos.
- Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs.
- Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados.
- Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo.
- Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.
- Deve permitir que o relatório seja enviado por e-mail para o destinatário específico.
- Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado.
- Deve permitir o uso de filtros nos relatórios.
- Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.
- Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.
- Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos.
- Deve permitir visualizar em tempo real os logs recebidos.
- Deve permitir o encaminhamento de log no formato syslog e no formato CEF (Common Event Format).
- Deve permitir gerar alertas de eventos a partir de logs recebidos.
- A solução deve possuir garantia, suporte e atualizações ao software durante 60 meses.

4.9. REQUISITOS GERAIS DO ITEM 03 (Appliance Físico ou virtual)

- A solução deve ser baseada em máquina virtual ou física do mesmo fabricante da solução de NGFW, e ter como objetivo
- gerenciar de modo centralizado todos os equipamentos a partir de uma única console de administração.
- A solução deve suportar (quando virtual):
- Deve ser compatível com os hypervisor VMWare 6.5 e superiores, Hyper-V 2016 e superiores.
- Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-ofsale.
- Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
- Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo.

- Permitir acesso concorrente de administradores, permitindo ainda que seja definida uma cadeia de aprovação das alterações realizadas.
- Possibilitar a criação e administração de políticas de firewall, controle de aplicação, sistema de prevenção a intrusão (IPS – Intrusion Prevention System), antivírus, filtro de URL.
- Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido.
- Permitir usar palavras chaves ou cores para facilitar identificação de regras.
- Permitir localizar em quais regras um objeto (ex. computador, serviço etc.) está sendo utilizado.
- Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS.
- Permitir criação de regras que fiquem ativas em horário definido.
- Realizar o backup das configurações para permitir o retorno de uma configuração salva.
- Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.
- Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas.
- Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora.
- Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota de maneira centralizada.
- Permitir criar os objetos que serão utilizados nas políticas de forma centralizada.
- Deve suportar a definição de perfis de acesso ao console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.
- Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, e TACACS+ .

4.10. REQUISITOS GERAIS DO ITEM 04

- Treinamento oficial sobre a solução de TIC como um todo envolvendo todos os itens da contratação, a ser ministrada aos colaboradores do MAPA (02 pessoas) que atuarão diretamente na administração e operação da solução após sua implementação, com carga horária mínima de 20 horas ou carga horária oficial. Obrigatoriamente, é necessário emitir certificado de participante para 02 pessoas e outros colaboradores que prestam serviço ao MAPA poderão participar do curso como ouvintes (No máximo serão 04 ouvintes).
- O treinamento deve iniciar em no máximo 10 dias úteis após a instalação e configuração da solução contratada ou a depender da disponibilidade do pessoal do MAPA.
- Os dias e horários para capacitação serão definidos pelo MAPA, conforme demanda do mesmo, podendo optar por utilizar apenas meio período do dia(ou até menos, se necessário) até completar a carga total prevista, e serão acordados com a contratada com uma antecedência mínima de 15 dias corridos antes do início do treinamento.
- O treinamento deverá abranger tanto teoria quanto exercícios práticos, voltados para conhecimento da arquitetura da solução, sua implantação, configuração/operação e gerenciamento, administração e monitoramento da solução, contemplando todos os aspectos essenciais de funcionamento, além de tratamento de problemas típicos envolvendo a operação da solução. Ademais, deve cobrir os seguintes tópicos: Arquitetura da solução; Configurações iniciais básicas; Alta disponibilidade; Controle de acesso dos administradores da solução; Configuração de Interfaces; Criação e gerenciamento de Zonas de Segurança, Políticas de Segurança e Endereçamento NAT; Controle por Identificação de Aplicações; Controle por Identificação de Usuários, com conexão a fontes externas de autenticação; Criação e gerenciamento de Filtro URL; noções gerais sobre a solução de armazenamento de logs e relatoria (item 02) e gerenciamento centralizado dos equipamentos (item 03), Descriptografia de tráfego; Configurações de VPN (SSL e IPSec); Monitoramento e Relatórios; ZTNA, Log e Auditoria.
- Deverá ser fornecido certificado a cada um dos servidores públicos participantes do treinamento. A apresentação destes certificados é requisito obrigatório para a comprovação da execução do serviço, sendo o principal artefato a ser utilizado pela equipe de fiscalização contratual para validação do serviço e emissão do Termo de Recebimento Definitivo da solução.
- Todo material didático a ser utilizado deverá ser fornecido pela contratada ou pelo fabricante, devendo esse ser umadocumentação oficial do próprio fabricante, impresso ou em PDF com todos os tópicos abordados no treinamento, inclusive com exemplos práticos e ilustrações.
- O instrutor deve ser profissional certificado pelo fabricante dos produtos e com experiência comprovada nos produtos fornecidos A critério do MAPA, o treinamento poderá ocorrer em:
    - Nas instalações do MAPA ou em outro local de Brasília-DF.
    - A contratada arcará com todas as despesas relativas e necessárias, tais como transporte, hospedagem e diárias do (s) instrutor(es); infraestrutura complementar da sala, instalações e equipamentos; material didático e coffee break, e demais gastos para a execução do treinamento.

4.11. REQUISITOS GERAIS DO ITEM 05

Deverá ter a característica de Zero Trust Network Access e funcionalidades para no mínimo usuários 400 simultâneos com os seguintes aspectos:

- Deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas.
- Deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão.
- Deve prover um método para controlar o acesso, identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust.
- A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário.
- Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem.
- O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante.
- Deve ser compatível com pelo menos os seguintes sistemas operacionais: Windows e Linux.
- Deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.2 e 1.3. Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários.
- A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso.
- Deve ser possível revogar o certificado de um agente por meio da console central.
- O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso.
- No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão.
- Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional.
- A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até 05 dias anteriores ao ocorrido.
- Deve existir a possibilidade de restringir o usuário de realizar backup da configuração do agente.
- Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes.
- A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4. Deve ser possível agrupar agentes em grupos e atribuir grupos de agentes a perfis de políticas específicas.
- Deve ser possível exigir uma senha para desconectar o agente da console central.
- Deve ser possível evitar que o usuário realize shutdown do agente após estar registrado na console central. A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA.
- Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas.
- A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa.
- Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais. Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente que não esteja em conformidade possa se conectar a redes críticas.
- A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda
- definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional. Além disso, deve ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows.

- Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar.

4.12. REQUISITOS DE ARQUITETURA TECNOLÓGICA

- Os requisitos de arquitetura tecnológica dos itens da contratação estão descritos ao longo do termo de referência e no **Anexo de Especificações técnicas da solução de TIC.**

4.13. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL E DE FORMAÇÃO DE EQUIPE

- Os profissionais que irão implantar a solução de TIC como um todo(Itens 01,02,03 e 05) devem ter experiência mínima de 03 anos em implantações/configurações da solução adquirida ou similar. Os atestados que comprovem essa experiência precisam ser apresentados formalmente. A contratada deve ter pelo menos 01(um) profissional, com certificação, certificado ou curso oficial do fabricante que comprove a aplicação prática em todos os itens da contratação.
- Já para o item 04 (treinamento) , o instrutor deve ter formação comprovada através de certificação/certificado ou curso oficial do fabricante e experiência em treinamentos de no mínimo 02 anos, devendo ser comprovado formalmente com documentos oficiais.

4.14. REQUISITOS DE METODOLOGIA DO TRABALHO

- A execução dos serviços está condicionada ao recebimento pela contratada da ordem de serviço (OS) emitida pelo MAPA. A OS indicará o serviço, a quantidade e a localidade na qual os serviços deverão ser prestados.
- A solução deverá estar implementada no prazo estabelecido neste termo de referência.
- A equipe do MAPA, no que couber, poderá apoiar a implantação da solução como um todo.
- Todos os serviços prestados pela contratada/subcontratada deverão ser realizados nas dependências do Ministério da Agricultura e Pecuária. A execução do serviço deve ser acompanhado pela contratada, que dará ciência de eventuais acontecimentos ao MAPA. Quando remoto, a infraestrutura necessária deve ser de responsabilidade da contratada.
- A contratada deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 8 horas por dia e 5 dias por semana de maneira eletrônica e 7 horas por dia e 5 dias por semana por via telefônica.
- A execução do contrato será baseada no modelo, no qual a contratante é responsável pela gestão do contrato e pelo ateste dos resultados esperados e dos níveis mínimos de serviço exigidos frente aos serviços entregues, sendo a contratada responsável pelos serviços, gestão dos recursos humanos e físicos necessários, conforme termo de referência.
- A contratada deverá se responsabilizar pelos materiais, produtos, ferramentas, instrumentos e equipamentos disponibilizados para a execução dos serviços, não cabendo à CONTRATANTE qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer.

4.15. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Na execução dos serviços contratados, a CONTRATADA deverá zelar, no que for de sua competência, pela garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações custodiadas no ambiente gerenciado. Além disso, deve adotar e se responsabilizar por medidas efetivas quanto ao seguinte:

- A contratada deverá submeter-se à Política de Segurança da Informação e Comunicações e demais normas de segurança vigentes no MAPA. (Portaria MAPA Nº 136, de 25 de Maio de 2021).
- Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca dos serviços, sem prévia autorização. Ademais, observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação - TI do MAPA.
- Normas e instruções normativas do GSI/PR no que se aplicar à respectiva contratação.
- Assegurar o adequado tratamento de dados pessoais e informações classificadas dos quais venha a ter conhecimento ou manusear em razão da execução do objeto do contrato, nos termos da Lei Federal n° 13.709/2018 e em aderência aos requisitos de segurança da informação vigentes no ambiente do MAPA.
- Evitar vazamento de dados e fraudes digitais nos ambientes gerenciados sob sua responsabilidade técnica.
- A contratada deverá assinar o termo de compromisso de manutenção de sigilo para fins de segurança de dados e da prestação do serviço, conforme o modelo no Anexo-Termo de compromisso de Manutenção de Sigilo (https://www.gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao).
- Os colaboradores da contratada que atuarem nos serviços iniciais e durante toda a vigência do contrato e do prazo de suporte e garantia, deverão assinar o termo de ciência, conforme o modelo no Anexo-Termo de Ciência (https://www.gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao).
- A contratada deverá obedecer, quando aplicável, as normas de segurança da família ISO/IEC 27000.

- A contratada deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, no que diz respeito a todo e qualquer assunto de interesse do MAPA ou de terceiros de que tomar conhecimento em razão da execução do objeto deste documento, devendo orientar seus empregados nesse sentido.
- A contratada deverá manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações de que vier ter acesso durante a execução do contrato.
- A contratada deverá implementar processo de gestão de capacidade e recursos para redundância de forma que a utilização dos recursos seja monitorada, ajustada e as projeções das necessidades de capacidade futura sejam avaliadas para garantir o desempenho dos ativos relacionados ao objeto do contrato, assegurando também a disponibilidade e recuperação de dados e informações, em conformidade com um plano de continuidade relacionado ao objeto contratado, que garanta o nível requerido de continuidade para a segurança da informação durante uma situação adversa; A contratada deverá manter controles e procedimentos específicos para assegurar o nível adequado de segurança da informação às redes corporativas da Contratante e da Contratada, de forma a reduzir o nível de risco ao qual a Solução de TIC e a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante.
- A contratada deverá implementar e manter controles específicos para registro de eventos e rastreabilidade de forma a manter trilha de auditoria de segurança da informação e privacidade, aderente a disposto em dispositivo legal correlato publicado pelo GSI/PR, de forma a assegurar a rastreabilidade do tráfego por meio de logs de transações e acessos, conforme especificação de requisitos, e gerá-los e disponibilizá-los à contratante para fins de auditorias e inspeções.
- A contratada deverá utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante;
- A contratada deverá implementar e manter controles e procedimentos específicos para assegurar completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da contratada venham a tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem o uso dos dados somente para as finalidades previstas em contrato e as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da Solução de TIC, cumprindo e fazendo cumprir o disposto nos Termo de Compromisso e Termo(s) de Ciência firmados respectivamente, pelo representante legal e pelo(s) empregado(s) da contratada.
- Todas as informações, documentos e especificações técnicas as quais a contratada tiver acesso em função da execução contratual deverão ser tratadas como confidenciais, sendo vedada sua reprodução, utilização ou divulgação à terceiros, devendo essa zelar pela manutenção do sigilo absoluto do conhecimento adquirido.

4.16. DEMAIS REQUISITOS APLICÁVEIS

- As empresas licitantes deverão apresentar declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio da competitividade e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto no art. 5º da Lei no 14.133, de 2021.
- Os demais requisitos envolvendo os itens da contratação estão elencados no Anexo de Especificação técnica da solução de TIC.

5. Modelo de execução do objeto

5. MODELO DE EXECUÇÃO DO OBJETO

O modelo de execução do contrato define como o contrato deverá produzir os resultados pretendidos desde o seu início até o seu encerramento, observando, os tópicos abaixo:

5.1 . CONDIÇÕES DE EXECUÇÃO E PROCEDIMENTOS DE FORNECIMENTO DA SOLUÇÃO DE TIC
5.1.1 . REUNIÃO INICIAL

Após a assinatura do contrato e a nomeação do gestores/fiscais de 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. A reunião será realizada em conformidade com o previsto no inciso I do artigo 31 da IN SGD/ME Nº94, de 2022, e ocorrerá em até 05 dias úteis da assinatura do contrato, podendo ser prorrogada a critério da contratante. A pauta desta reunião observará, pelo menos:

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

- Alinhar a forma de comunicação entre as partes, que deverá ocorrer preferencialmente entre o MAPA e o preposto da contratada.
- Definir as providências necessárias para inserção da contratada no ambiente de prestação dos serviços.
- Definir as providências de implantação dos serviços.
- Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.
- Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.
- Apresentação formal da equipe de fiscalização do contrato e do preposto. (contratante e contratada)
- Repasse à contratada de conhecimentos necessários à execução dos serviços (contratante).
- Entrega, por parte da contratada, do termo de compromisso e dos termos de ciência devidamente assinados, conforme artigo 18, inciso V da IN SGD/ME Nº 94/2022.

Havendo necessidade outros assuntos de comum interesse, poderão ser tratados na reunião inicial, além dos anteriormente previstos. Todas as atas de reuniões e as comunicações entre o MAPA e a contratada, assim como todas as demais intercorrências contratuais, positivas ou negativas, serão arquivadas em processo próprio para fins de manutenção do histórico de gestão do contrato.

5.1.2 . PRAZOS, HORÁRIOS DE FORNECIMENTO DE BENS/PRESTAÇÃO DE SERVIÇOS E LOCAIS DE ENTREGA

Além dos prazos já citados nos requisitos temporais, outros prazos devem ser cumpridos:

ID	DESCRIÇÃO	PRAZO MÁXIMO DE ENTREGA (DIAS ÚTEIS)
01	Assinatura do contrato.(MAPA e Contratada)	Início dos prazos - D
02	Realização da reunião inicial contendo os elementos descritos no item 651.1 deste termo de referência. (MAPA e contratada).	05 dias úteis após o ID 1.
03	Entrega do projeto da implantação (Contratada).	05 dias úteis após o ID 2.
04	Análise e aprovação do projeto de implantação (contratante).	05 dias úteis após o ID 3.
05	Finalização da execução dos serviços e instalação dos bens. (Contratada)	60 dias úteis após o ID 4.
06	Início do treinamento.	10 dias após o ID 5 ou a depender da disponibilidade dos recursos do MAPA.
07	Termo de Recebimento Provisório.	05 dias após a finalização do ID 5 e ID 06.
08	Termo de Recebimento Definitivo.	10 dias após a finalização do treinamento e ID 07.
09	Relatórios mensais a partir do 2º mês de instalação com o detalhamento das manutenções preventivas.	Todo 5º dia útil do mês subsequente.

- O local para fornecimento dos bens físicos e prestação dos serviços é Brasília- Distrito Federal, Esplanada dos Ministérios, Ministério da Agricultura e Pecuária-MAPA, Anexo "B" e térreo.
- A entrega dos equipamentos físicos deverão ser realizados nos dias úteis, no horário de 09:00 às 12:00 e de 14:00 às 17: 00, devendo ser agendada previamente com o MAPA.
- O transporte dos equipamentos deverá ser realizado pela contratada, inclusive os procedimentos de seguro, embalagem e transporte até o espaço alocado pelo MAPA para guarda.
- Caberá ao MAPA rejeitar no total ou em parte, os materiais entregues em desacordo com o objeto deste Termo de Referência.
- O recebimento da solução de TIC será efetivado pela equipe designada pelo MAPA e dar-se-á da forma provisória e definitiva, conforme prazos estabelecidos no tópico 7.6.2 deste termo de referência.
- Caso não seja possível conclusão do item 05 no tempo previsto, a empresa deverá comunicar as razões respectivas com pelo menos 10 dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

5.1.3 . DOCUMENTAÇÃO MÍNIMA EXIGIDA

No mínimo, a Contratada deverá fornecer:

- Manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração.

- Documentação completa de todos os itens da contratação, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas;
- Relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.
- Relatórios mensais das manutenções preventivas, relatórios dos tickets executados e seu cumprimento com os níveis mínimos de serviço.

5.1.4 . PAPÉIS E RESPONSABILIDADES, POR PARTE DO CONTRATANTE E DA CONTRATADA
Os papéis a serem designados e necessários para essa contratação estão descritos no item 7.7.4 deste termo de referência.

5.1.5 . MATERIAIS A SEREM DISPONIBILIZADOS
Para a perfeita execução dos serviços, a contratada é responsável por todos os materiais, equipamentos, ferramentas e utensílios necessários para a instalação e configuração dos bens adquiridos.

5.1.6 . INFORMAÇÕES RELEVANTES PARA O DIMENSIONAMENTO DA PROPOSTA
A demanda do órgão tem como base as seguintes características: manter a mesma arquitetura atual de firewall (a topologia está omitida por segurança) e substituir os equipamentos atuais (08 Firewalls. 02 Aker 12137 e 06 Aker 8137).

5.2. QUANTIDADE DE BENS A SEREM FORNECIDOS
A quantidade de bens e serviços a serem fornecidos estão descritos e justificado em detalhes no item 3.4 desse termo de referência e em outros tópicos do mesmo.

5.3. MECANISMOS FORMAIS DE COMUNICAÇÃO

- Toda comunicação entre o MAPA e a contratada deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro meio de comunicação.
- Na reunião inicial, a Contratada deverá indicar formalmente preposto apto a representá-la junto ao MAPA. Esse profissional fará a interação entre o MAPA e a Contratada, e será responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao Contratante.
- Os seguintes instrumentos formais poderão ser utilizados para a troca de informações entre a Contratante e a Contratada, sendo eles: Ordem de Serviço e ofícios enviados via SEI, Ata de Reunião, Canal de abertura de chamados, E-mails, Ferramentas de colaboração da Microsoft, por exemplo, Teams ou outra que venha a utilizada pelo MAPA, de acordo com a natureza da informação.

Algumas das comunicações corriqueiras podem ser exemplificadas abaixo:

- Exemplo de comunicação 01: Autorizar a execução dos serviços, fornecimento de bens ou entrega das Licenças.
  - Documento: Ordem de Serviço.
  - Emissor: Contratante – Gestor do Contrato e Fiscal Requisitante.
  - Destinatário: Contratada.
  - Meio: eletrônico.
- Exemplo de comunicação 02: Abertura de chamados de suporte técnico e garantia.
  - Documento: Solicitação de abertura de chamado de suporte técnico e garantia.
  - Emissor: Contratante.
  - Destinatário: Contratada.
  - Meio: E-mail, telefone ou site na internet.
- Exemplo de comunicação 03: Registro das reuniões realizadas entre o Contratante e a Contratada.
  - Documento: Ata de reunião.
  - Emissor: Contratada.
  - Destinatário: Contratante.
  - Meio: eletrônico.
- Exemplo de comunicação 04: Dirimir dúvidas e prestar esclarecimentos acerca de itens presentes no contrato firmado.
  - Documento: Ofício e/ou relatório mensal.
  - Emissor: Contratada ou contratante.
  - Destinatário: Contratada ou contratante.
  - Meio: eletrônico com confirmação de recebimento.

5.4. MANUTENÇÃO DE SIGILO E NORMAS DE SEGURANÇA
5.4.1 . TERMO DE COMPROMISSO / TERMO DE CIÊNCIA DA DECLARAÇÃO DE MANUTENÇÃO DE SIGILO E DAS NORMAS DE SEGURANÇA NO MAPA

- A Contratada 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 dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

- 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 da Contratada, e Termo de Ciência , a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos anexos.

5.5 . FORMA DE TRANSFERÊNCIA DE CONHECIMENTO

- A transferência do conhecimento se dará através do item 05(Treinamento) desta contratação e possíveis reuniões apresentadas pela equipe que fez a instalação/configuração dos equipamentos.

5.6 . PROCEDIMENTOS DE TRANSIÇÃO E FINALIZAÇÃO DO CONTRATO

- Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto. Caso o MAPA sinta necessidade de solicitação de qualquer outra informação importante durante o contrato, não deve haver recusa da contratada em fornecê-la.

5.7. PAPÉIS E RESPONSABILIDADES

As responsabilidades do contratante e da contratada seguem abaixo:

5.7.1. DEVERES E RESPONSABILIDADES DO CONTRATANTE

- Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução do contrato;
- Encaminhar formalmente a demanda, preferencialmente por meio de Ordem de Serviço, de acordo com os critérios estabelecidos neste Termo de Referência.
- Receber o objeto/serviço fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.
- Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do presente Termo de Referência e da proposta da contratada, para fins de aceitação e recebimento definitivo;
- Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;
- Aplicar, observando o direito ao contraditório e ampla defesa, à contratada as sanções administrativas regulamentares e contratuais cabíveis.
- Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato.
- Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da Solução de Tecnologia da Informação.
- Disponibilizar para a contratada: legislação, normas, instruções e programas de trabalho de sua competência, com o objetivo de facilitar e orientar a execução dos serviços contratados.
- Permitir à contratada os acessos a todas as áreas, instalações e equipamentos necessários ao cumprimento das tarefas e serviços previstas neste Termo de Referência.
- Prestar à contratada, em tempo hábil, as informações disponíveis e necessárias à implantação/execução dos serviços.
- Exigir, a qualquer tempo, a comprovação das condições de habilitação da contratada que ensejaram sua contratação.
- Manter a contratada informada de quaisquer atos da Administração Pública que venham a interferir direta ou indiretamente nos serviços contratados.
- Por se tratar de solução de tecnologia da informação, todas as obrigações da contratante contidas na IN SGD/ME 94 /2022 deverão ser seguidas, incluindo a emissão do TRP (Termo de Recebimento Provisório) e o TRD (Termo de Recebimento Definitivo).

5.7.2. DEVERES E RESPONSABILIDADES DA CONTRATADA

- Executar os serviços e iniciar a cobertura e a execução dos serviços conforme especificações deste Termo de Referência e de sua proposta comercial, com a disponibilidade dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, na qualidade e quantidade especificadas.
- Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade.
- O objeto deve estar acompanhado do manual do usuário, com uma versão em português do Brasil ou inglês.
- Responsabilizar-se pelos vícios e danos decorrentes da execução dos objetos, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos.
- Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor.

- Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010.
- Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade ao Contratante.
- Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração.
- Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a Contratada relatar à Contratante toda e qualquer ocorrência neste senti do, a fim de evitar desvio de função.
- Relatar ao Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.
- Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato.
- Manter-se, durante toda a execução do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para a contratação.
- Responsabilizar-se integralmente pelo fiel cumprimento dos objetos contratados, prestando todos os esclarecimentos eventualmente solicitados pela contratante, obedecendo aos parâmetros e rotinas estabelecidos de acordo com as recomendações aceitas pela boa técnica, normas e legislação vigentes.
- Executar o objeto contratado conforme as condições estipuladas neste Termo de Referência e seus Anexos, na Proposta Comercial e no Contrato.
- Indicar formalmente, no período designado pelo termo de referência, preposto e substituto aptos a representá-la junto a Contratante, os quais devem responder pela fiel execução dos serviços contratados, orientar a Equipe da Contratada, bem como comparecer às dependências da Contratante sempre que convocados.
- Não transferir a outrem, no todo ou em parte, a execução do presente Contrato.
- Atender às solicitações dos membros da Equipe de Gestão do Contrato inerentes às obrigações contratuais e/ou à prestação e/ou à gestão dos serviços.
- Comunicar formal e imediatamente ao Gestor do Contrato todas as ocorrências anormais ou de comprometimento à execução do Contrato, bem como qualquer ocorrência relevante à execução contratual.
- Efetuar de imediato o afastamento do atendimento à Contratante de qualquer empregado cuja atuação, permanência ou comportamento sejam inadequados à execução do Contrato.
- Responsabilizar-se por quaisquer encargos, despesas, taxas, inclusive de seguro, decorrentes das operações necessárias à entrega do objeto contratado.
- Reparar quaisquer danos diretamente causados à Contratante ou a terceiros, por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da presente relação contratual, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução dos serviços pela Contratante.
- Observar todas as normas de segurança adotadas pelo Contratante, inclusive no que diz respeito às normas referentes ao ambiente informatizado.
- Fornecer ao Contratante, sempre que requerido formalmente, acesso aos equipamentos e sistemas necessários ao atendimento do objeto do Contrato, para averiguação da conformidade dos serviços contratados.
- Cumprir as disposições do Termo de Compromisso de Sigilo e do Termo de Ciência.
- Responsabilizar-se por todos os custos, diretos e indiretos, inclusive de transporte e de pessoal, necessários à adequada prestação dos serviços, em plena conformidade com os termos e especificações, inclusive prazos e horários previstos neste Termo de Referência e seus anexos.
- Assegurar a disponibilidade, confidencialidade e integridade dos dados, informações e sistemas informatizados, inclusive de todas as suas alterações, manuais, programas fonte e objeto, bases de dados ou outros recursos, pertencentes ao Contratante, armazenados ou residentes na Contratada.
- Registrar, tempestivamente, mediante relatório circunstanciado, todos os casos que a eximam de responsabilidade, negligência, mau uso, instalações e outros.
- Propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária.
- Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários até 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato;
- Apresentar fatura no valor autorizado e condições do Contrato, apresentando-a ao Contratante para ateste e pagamento após a autorização de faturamento pelo Gestor do Contrato.
- Atender as determinações do Gestor do Contrato inerentes às obrigações contratuais e/ou à prestação e/ou gestão dos serviços.
- A Contratada não poderá divulgar projetos, serviços e soluções de TIC do MAPA e Ministérios demandantes, nem falar em nome do Contratante em nenhum tipo de mídia sem prévia autorização.
- Não disponibilizar qualquer informação de propriedade do Contratante, por qualquer meio, a qualquer terceiro e para qualquer finalidade, sem anuência expressa.
- 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, sendo assim o caso, incluindo a documentação, os modelos de dados e as bases de dados à Administração.

- Assumir as despesas decorrentes do transporte, hospedagem e alimentação a ser executado em função do objeto do Contrato.
- Diante de situações de irregularidades de caráter urgente deverá comunicar, por escrito, ao Contratante, as informações sobre possíveis paralisações de serviços, a apresentação de relatório técnico ou razões justificadoras a serem apreciadas e decididas pelo agente designado.
- Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).
- Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da contratante.
- Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão.
- Indicar formalmente e por escrito, no prazo máximo de 05 dias úteis após a assinatura do contrato, junto à contratante, um preposto idôneo com poderes de decisão para representar a contratada, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato.
- Em até 48 horas corridas, devem ser enviadas informações dos funcionários desligados que estejam prestando serviço ao MAPA.

6. Modelo de gestão do contrato

6. MODELO DE GESTÃO DO CONTRATO

6.1. - 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.
6.2. - 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.
6.3. - 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.
6.4. - O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. FISCALIZAÇÃO CONTRATUAL

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, no que for necessário, observando-se, em especial, as rotinas a seguir:

6.5.1. FISCALIZAÇÃO TÉCNICA

- 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).
- O fiscal técnico do contrato anotará 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).
- 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);
- 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).
- 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).
- 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).

6.5.2. FISCALIZAÇÃO ADMINISTRATIVA

- 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).
- 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).

6.5.3. GESTOR DO CONTRATO

- 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).
- 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).
- 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).
- 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).
- 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).
- 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).
- O gestor do contrato deverá elaborará 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. Critérios de medição e pagamento

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

7.1. CRITÉRIOS DE ACEITAÇÃO DOS BENS FORNECIDOS

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

- 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 recondicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).
- Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si e do mesmo fabricante, conforme já dito ao longo do termo de referência, 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.
- O número de série(part numbers e modelos) 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.
- 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.

- 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.
- A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou será realizada verificação de amostra do objeto para averiguar se a Solução de TIC apresentada pela Licitante detém os requisitos mínimos necessários para realização dos serviços a serem contratados, de acordo com as funcionalidades, procedimentos e critérios objetivos descritos termo de referência e seus respectivos anexos.
- 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 objeto 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.

Qualquer item da contratação será recusada inteiramente nas seguintes condições:

- Caso seja entregue em desconformidade com as especificações técnicas constantes deste Temo de Referência e da proposta vencedora;
- Caso apresente defeitos, em qualquer de suas partes ou componentes, durante os testes de conformidade e verificação;
- Nos casos de recusa do produto, a empresa fornecedora terá o prazo de 05 (cinco) dias úteis para providenciar a sua substituição, contados a partir da comunicação oficial feita pelo MAPA.

7.2. RECEBIMENTO DO OBJETO

O objeto contratado será recebido, de forma provisória e definitiva, conforme prevê o artigo 140 da Lei Nº 14.133 e o art. 33 da Instrução Normativa N° 23/2022/SGD/ME, observando o disposto a seguir:

7.2.1. TERMO DE RECEBIMENTO PROVISÓRIO

- Os serviços serão recebidos provisoriamente, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.
- O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços e bens a que se referem a parcela a ser paga.
- 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).
- 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) 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.
- O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.
- Os serviços e bens 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.
- 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.

7.2.1. TERMO DE RECEBIMENTO DEFINITIVO

Os serviços serão recebidos definitivamente no prazo de 10 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:

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

- Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.
- 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.
- Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.
- 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.
- 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 objeto 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.
- 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.

7.3 . PROCEDIMENTOS DE TESTE E INSPEÇÃO

7.3.1 . DEFINIÇÃO DE MECANISMOS DE INSPEÇÃO E AVALIAÇÃO DA SOLUÇÃO / DILIGÊNCIAS

O acompanhamento e a fiscalização do objeto deste Termo de Referência, bem como o atesto da entrega dos materiais adquiridos, serão exercidos por servidor , em conformidade com o disposto no art. 117 da Lei n.º 14.1333 e com as normas e resoluções internas do Órgão. O acompanhamento e a fiscalização serão realizados sob o aspecto quantitativo e qualitativo, devendo ser anotadas em registro próprio dos fiscais as falhas detectadas.

As irregularidades detectadas pela fiscalização serão imediatamente comunicadas ao fornecedor, por escrito, para correção ou adequação.

7.3.2 . ORIGEM E FORMAS DE OBTENÇÃO DAS INFORMAÇÕES NECESSÁRIAS À GESTÃO E FISCALIZAÇÃO DO CONTRATO / ACOMPANHAMENTO DE INDICADORES

- A origem das informações necessárias à gestão e fiscalização do contrato serão as comunicações entre o preposto e a equipe de fiscalização técnica do contrato. Todas as demais informações geradas ao longo do contrato também servem de base para a fiscalização contratual.
- Não é necessário nenhum software específico para acompanhar os indicadores, sendo os relatórios e plataforma de abertura de tickets suficientes para uma fiscalização contratual eficaz.

7.3.3 . DEFINIÇÃO DE LISTAS DE VERIFICAÇÃO E DE ROTEIROS DE TESTES PARA SUBSIDIAR A AÇÃO DOS FISCAIS DO CONTRATO

- O MAPA reserva-se ao direito de promover avaliações, inspeções e diligências visando esclarecer quaisquer situações relacionadas à prestação dos serviços contratados, sendo obrigação da contratada acolhê-las.
- A inspeção nos equipamentos fornecidos será realizada por meio de comparação das especificações constantes dos prospectos do fabricante do equipamento.

7.3.4 . DISPONIBILIDADE DE RECURSOS HUMANOS NECESSÁRIOS ÀS ATIVIDADES DE GESTÃO E FISCALIZAÇÃO DO CONTRATO / PAPÉIS E RESPONSABILIDADES, POR PARTE DO CONTRATANTE E DA CONTRATADA

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 artigo 33 da IN SGD Nº 94 de 2022, e para cumprir as atividades de gestão e fiscalização do contrato, o MAPA designará servidores (titulares e substitutos) para executar os seguintes papéis:

7.3.4.1. - DO CONTRATANTE-MAPA

Gestor do Contrato: Servidor com atribuições gerenciais, preferencialmente da Área Requisitante da solução, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente. Outras atribuições estão listadas no inciso I do artigo 33 da IN SGD/ME Nº 94/2022.

Fiscal Técnico: Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato. Outras atribuições estão listadas no inciso II do artigo 33 da IN SGD /ME Nº 94/2022.

Fiscal Requisitante: Servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação. Outras atribuições estão listadas no inciso III do artigo 33 da IN SGD/ME Nº 94/2022.

Fiscal administrativo: Servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos. Outras atribuições estão listadas no inciso IV do artigo 33 da IN SGD /ME Nº 94/2022.

7.3.4.2. - DA CONTRATADA

Preposto: Representante da contratada, responsável por 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. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

Profissionais da Contratada: Funcionário(s) representante(s) da contratada, responsável(is) por executar as atividades /serviços contratados.

7.4 . PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO

7.4.1 . NÍVEIS MÍNIMOS DE SERVIÇO/INDICADORES

Para permitir que a gestão contratual esteja alinhada com a gestão da qualidade dos serviços prestados, foram estabelecidos indicadores de desempenho mínimos para a execução dos serviços contratados. Assim, os resultados serão medidos com base em indicadores vinculados a fórmulas de cálculo específicas, apurados temporalmente e continuamente monitorados, objetivando o cumprimento das metas estabelecidas. Este conceito vincula-se ao novo modelo de contratação de soluções de Tecnologia da Informação na Administração Pública Federal, no qual os serviços serão remunerados considerando parâmetros de qualidade e entrega efetiva de resultados.

Os indicadores são instrumentos práticos de aferição do cumprimento do alcance dos níveis mínimos de serviço, evidenciando de maneira objetiva e mensurável o desempenho e as tendências de um serviço demandado. Relaciona-se a seguir o conjunto mínimo de indicadores proposto para a presente contratação, pautado no incentivo para a redução de ocorrências que impactam o negócio do MAPA e também incentivem a boa prestação dos serviços:

INDICADOR A	
TÓPICO	**DESCRIÇÃO**
Finalidade	Este indicador tem a finalidade de medir a carga horária completa do treinamento.
Meta a cumprir	Atender 100% da carga horária mínima do treinamento.
Instrumento de medição	Recebimento dos certificados pelo equipe de fiscalização contratual.
Periodicidade	Única.
Glosa	Redução de 5% sobre o valor do item 5 a cada 1 hora menor de treinamento.

INDICADOR B	
Finalidade	Este indicador tem a finalidade de verificar a data de entrega dos bens e principais itens da solução de TIC.
Meta a cumprir	Atender 100% das datas máximas de cada item descrito na tabela dos requisitos temporais).
Instrumento de medição	Através das datas iniciais e finais de execução de cada item.
Periodicidade	Única
Glosa	Glosa de 0,25% por dia de atraso sobre o valor total do contrato, caso qualquer ID tenha sua data máxima extrapolada.

7.4.2. NÍVEIS DE SEVERIDADE DOS CHAMADOS EM GARANTIA

Os chamados abertos envolvendo garantia e manutenção deverão ser atendidos conforme os índices de criticidade abaixo:

CRITICIDADE	**DESCRIÇÃO DA ATIVIDADE/SERVIÇO**	**PRAZO MÁXIMO PARA SOLUÇÃO DO PROBLEMA**
MÁXIMA	Chamados referentes a situações de urgência ou problema crítico, caracterizados pela existência de ambiente paralisado, com equipamentos parcialmente ou totalmente inoperantes e/ou que envolvam paralisações ou severa perda de desempenho nos serviços, inclusive aqueles que envolvam a troca do equipamento.	08 horas úteis após a abertura do chamado.

ALTA	Chamados associados a situações de alto impacto, referentes ao uso do produto, com equipamentos parcialmente ou totalmente inoperantes e/ou que envolvam paralisações ou severa perda de desempenho nos serviços, inclusive aqueles que envolvam a troca do equipamento.	16 horas úteis após a abertura do chamado.
NORMAL	Chamados com o objetivo de sanar dúvidas quanto ao uso ou à implementação do produto, que não envolvam paralisações ou severa perda de desempenho nos serviços, ou que não impliquem em equipamentos ou módulos de equipamentos total ou parcialmente inoperantes.	28 horas úteis após a abertura do chamado.
A definição de prazos máximos para início de atendimento não são necessárias. O foco é em resolver o problema e em quanto tempo, não sendo necessário estimar em quanto tempo terá início para atendimento do ticket. O tipo de atendimento pode ser remoto/presencial, de acordo com a natureza do problema.		

7.4.3. PROCEDIMENTOS PARA APLICAÇÃO DE GLOSA NO PAGAMENTO

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:

- Não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou
- Deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada.

A aplicação de descontos/glosas em função do descumprimento de critérios de qualidade, avaliação de resultados e/ou níveis mínimos de serviço exigidos não concorre com a aplicação (concomitante ou não) das sanções administrativas previstas em contrato, inclusive daquelas previstas em função do reiterado descumprimento dos critérios de qualidade do serviço, sendo essa uma prerrogativa da Administração.
Além das reduções de valores relacionados aos indicadores, serão aplicadas glosas em função das pontuações diretamente atribuídas ao descumprimento dos termos de serviço determinados da tabela abaixo, sendo as ocorrências apuradas, sempre que necessário. As glosas serão aplicadas sem prejuízo de outras sanções administrativas por descumprimento de obrigações contratuais e estão incluídas no limite máximo de 30% do pagamento à contratada.

REDUÇÃO NO PAGAMENTO DE ACORDO COM OS REQUISITOS GERAIS DO TERMO DE REFERÊNCIA			
ID	**DESCRIÇÃO**	**REFERÊNCIA**	**GLOSA**
01	Não utilizar mão de obra qualificada e tecnicamente habilitada para o atendimento.	Por ocorrência.	1ª ocorrência - Glosa de 0,25% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,5% sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% sobre o valor total do contrato.
02	Deixar de comunicar qualquer anormalidade técnica de caráter urgente para o contratante.	Por ocorrência.	1ª ocorrência - Glosa de 0,50% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,75% sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% sobre o valor total do contrato.
03	Não comparecer, injustificadamente, à reunião inicial.	Por ocorrência.	1ª ocorrência - Glosa de 0,25% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,5% sobre o valor total do contrato.
04	Provocar a indisponibilidade dos equipamentos ou comprometer a confidencialidade, integridade	Por ocorrência.	1ª ocorrência - Glosa de 0,50% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,75%

	e indisponibilidade da solução.		sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% sobre o valor total do contrato.
05	Deixar de cumprir os requisitos de segurança.	Por ocorrência.	1ª ocorrência - Glosa de 0,50% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,75% sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% sobre o valor total do contrato.
06	Não substituir qualquer equipamento da solução de TIC nos prazos máximos especificados.	Por ocorrência.	1ª ocorrência - Glosa de 0,50% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,75% sobre o valor total do contrato. 3ª ocorrência - Glosa de 2,0% sobre o valor total do contrato.
07	Não entregar e não cumprir 100% das atividades de manutenção preventiva mensal.	Por ocorrência.	1ª ocorrência - Glosa de 0,35% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,55% sobre o valor total do contrato. 3ª ocorrência - Glosa de 1,0% sobre o valor total do contrato.
08	Não atender 96% dos tickets de todas as severidades atendidos dentro do prazo mensalmente.	Por ocorrência.	1ª ocorrência - Glosa de 0,25% sobre o valor total do contrato. 2ª ocorrência - Glosa de 0,5% sobre o valor total do contrato. 3ª ocorrência - Glosa de 0,75% sobre o valor total do contrato.

7.5. SANÇÕES ADMINISTRATIVAS

A finalidade das sanções administrativas em licitações e contratos é reprovar a conduta praticada pelo sancionado, desestimular a sua reincidência, bem como prevenir sua prática futura pelos demais licitantes e contratados. As sanções podem ter caráter preventivo, educativo, repressivo ou visar à reparação de danos pelos responsáveis que causem prejuízos ao erário público. Trata-se, portanto, de um poder-dever da Administração que deve atuar visando impedir ou minimizar os danos causados pelos licitantes e contratados que descumprem suas obrigações.
As reduções previstas no período de adaptação não se estendem para as hipóteses de aplicação de sanções. As sanções administrativas fixadas nas normas, aplicadas aos licitantes e contratada, são as seguintes:
A) Advertência. B) Multa. C) Impedimento de licitar e contratar. D) Declaração de inidoneidade para licitar ou contratar.
As sanções “advertência”, “impedimento de licitar e contratar” e “declaração inidoneidade ou contratar” poderão ser aplicadas cumulativamente com a sanção de multa.

7.5.1. ADVERTÊNCIA

A sanção de advertência será aplicada exclusivamente pela infração administrativa prevista no inciso I do caput do art. 155 desta Lei Nº 14.1333, quando não se justificar a imposição de penalidade mais grave.

7.5.2. MULTA

A sanção de multa tem natureza pecuniária e sua aplicação se dará na gradação prevista neste instrumento quando houver atraso injustificado no cumprimento da obrigação contratual e em decorrência da inexecução parcial ou total do objeto da contratação nos termos do artigo 162 da Lei Nº 14.133. As sanções de advertência, suspensão e inidoneidade poderão ser aplicadas juntamente com a multa, conforme § 7º do art. 156 de Lei nº 14.133. As MULTAS serão aplicadas considerando os seguintes níveis de gradação:

GRAU DE INFRAÇÃO	**GRAVIDADE**	**MULTA CORRESPONDENTE**	**LIMITE DE INFRAÇÕES POR VIGÊNCIA CONTRATUAL**
INFRAÇÃO A	Conduta indesejada com baixo impacto na realização dos objetivos da contratação.	0,5% sobre o valor global do contrato.	Até 06 (seis) infrações, consecutivas ou não.
	Conduta prejudicial, impacta		

INFRAÇÃO A	a prestação dos serviços de maneira leve, mas não compromete a realização dos objetivos da contratação.	1,0% sobre o valor global do contrato.	Até 04 (quatro) infrações, consecutivas ou não.
INFRAÇÃO A	Conduta danosa, impacta a prestação dos serviços de maneira mediana ou compromete a realização dos objetivos da contratação.	2,5% sobre o valor global do contrato.	Até 02 (duas) infrações, consecutivas ou não.
INFRAÇÃO A	Conduta grave, compromete fortemente a realização dos objetivos da contratação.	3,5 % sobre o valor global do contrato.	Até 01(uma) infração.
Importante: Ao exceder o limite máximo admitido de infrações durante a vigência contratual para o respectivo nível de gradação estabelecido, ou mediante o reiterado descumprimento de critérios de qualidade e/ou níveis mínimos de serviço exigidos, o MAPA deverá avaliar a possibilidade de promover a rescisão do contrato em função da inexecução total ou parcial do objeto, da perda de suas funcionalidades e da comprovada desconformidade com os critérios mínimos de qualidade exigidos – ressalvada a aplicação adicional de outras sanções administrativas cabíveis.			

A contratada estará sujeita à aplicação de multa, de acordo com os respectivos níveis de gradação acima descritos, quando for observada a ocorrência dos seguintes eventos:

EVENTOS DE REFERÊNCIA PASSÍVEIS		
ID	**DESCRIÇÃO DO EVENTO INFRACIONAL**	**GRAU DA INFORMAÇÃO**
01	Dar causa à inexecução parcial do contrato.	Infração B
02	Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo.	Infração C
03	Dar causa à inexecução total do contrato.	Infração D
04	Deixar de entregar a documentação exigida para o certame.	Infração B
05	Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado.	Infração B
06	Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta.	Infração C
07	Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado.	Infração C
08	Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato.	Infração D
09	Fraudar a licitação ou praticar ato fraudulento na execução do contrato.	Infração D
10	Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza.	Infração D
11	Praticar atos ilícitos com vistas a frustrar os objetivos da licitação.	Infração D
12	Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.	Infração D

7.5.3. IMPEDIMENTO DE LICITAR E CONTRATAR

A sanção prevista será aplicada ao responsável pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do do art. 155 Da Lei Nº 14.133, quando não se justificar a imposição de penalidade mais grave, e impedirá caput o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos.

7.5.4. DECLARAÇÃO DE INIDONEIDADE PARA LICITAR E CONTRATAR

A sanção prevista será aplicada ao responsável pelas infrações administrativas previstas nos incisos VIII, IX, X, XI e XII do caput do art. 155 da Lei Nº 14.133, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do caput do artigo 156 que justifiquem a imposição de penalidade mais grave que a sanção referida no § 4º deste mesmo artigo,

e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.
A sanção de "Declaração de inidoneidade para licitar ou contratar" será precedida de análise jurídica e observará as seguintes regras:
I - quando aplicada por órgão do Poder Executivo, será de competência exclusiva de ministro de Estado, de secretário estadual ou de secretário municipal e, quando aplicada por autarquia ou fundação, será de competência exclusiva da autoridade máxima da entidade.

7.6. LIQUIDAÇÃO

- Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de trinta 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.
- 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:
    - O prazo de validade;
    - A data da emissão;
    - Os dados do contrato e do órgão contratante;
    - O período respectivo de execução do contrato;
    - O valor a pagar; e
    - Eventual destaque do valor de retenções tributárias cabíveis.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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. 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.

7.7. PRAZO DE PAGAMENTO

- O pagamento será efetuado no prazo de até 30 dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.
- 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 de correção monetária através da seguinte fórmula:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX)$$
$$I = (6 / 100) / 365$$
$$I = 0,00016438$$

TX = Percentual 365 da taxa anual = 6%.

7.8. FORMA DE PAGAMENTO

- Todos os itens da contratação serão pagos depois da execução, de forma única, comprovação e fiscalização dos serviços, após o Termo de recebimento definitivo, em parcela única.
- O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.
- Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
- 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.
- 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.
- Comunicar a empresa para emissão de Nota Fiscal no que pertinente à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021.
- O valor relativo à parcela antecipada(caso seja necessário) e não executada do contrato será atualizado monetariamente pela variação acumulada do ICTI, ou outro índice que venha a substituí-lo, desde a data do pagamento da antecipação até a data da devolução.
- A liquidação ocorrerá de acordo com as regras do tópico respectivo deste instrumento.
- O pagamento será efetuado no prazo máximo de até 30 dias contados do recebimento do recebimento da nota fiscal.
- 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.
    - As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.

8. Critérios de seleção do fornecedor

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

8.1. REGIME E MODALIDADE DA CONTRATAÇÃO

- A contratação para execução indireta de serviços será realizada pelo regime de “empreitada por preço global”, quando se contrata a execução da obra ou do serviço por preço certo e total – conforme descrito na alínea a do inc. II do artigo 46 da Lei Nº 14.133.
- A adjudicação por preço global se deve ao fato de que todos os equipamentos e serviços estão intrinsecamente relacionados. A execução dos serviços por mais de uma empresa acarretaria elevado custo de administração e uma complexa rede de coordenação entre os projetos e, certamente, comprometeria a qualidade e efetividade dos resultados para o MAPA. A divisão do objeto a ser licitado em itens pode acarretar prejuízos quanto à instalação, configuração e operacionalização de todo o sistema, bem como sua manutenção, uma vez que se exige total compatibilidade entre os equipamentos da solução a ser adquirida, ou seja, a instalação tem que ser uniforme.
- O Item levou em consideração questões técnicas, sem prejuízo a ampla competitividade, uma vez que existem no mercado várias empresas com capacidade de fornecer os produtos na forma em que estão agrupados neste TR.
- Ademais, não será aplicado o disposto no Art. 8º do Decreto nº 8.538 de 06 de outubro de 2015, considerando a inviabilidade técnica e econômica para o parcelamento do objeto da presente contratação, bem como consideradas as suas respectivas peculiaridades, interdependência e natureza acessória entre as parcelas do objeto.

8.2. NATUREZA DOS SERVIÇOS

- Os serviços a serem contratados enquadram-se nos pressupostos do Decreto Nº 9.507 de 21 de Setembro de 2018, constituindo-se em “ serviços auxiliares, instrumentais ou acessórios ” à área de competência legal do órgão licitante, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.
- Ainda, o objeto deste termo de referência se caracteriza como serviço de natureza continuada em função da sua essencialidade e habitualidade para o MAPA, ou seja, uma eventual paralisação desses serviços pode implicar sérios prejuízos às atividades do MAPA. Nos termos do art. 15 da IN 05/SEGES/MPDG de 26/05/2017, “os serviços prestados de forma contínua são aqueles que, pela sua essencialidade, visam atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público ou o funcionamento das atividades finalísticas do órgão ou entidade, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional”.

- Quanto ao tipo de serviço, em conformidade com a lei Nº 14.133, com o Decreto n° 5.450/2005 e com o art. 14 da IN 05 /SEGES/MPDG de 26/05/2017, o objeto pretendido enquadra-se como “Serviço comum” por apresentar, independentemente de sua complexidade, “padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado”.
- Por fim, a prestação de serviços não envolve “dedicação exclusiva de mão de obra” – nos termos do art. 17 da IN 05 /SEGES/MPDG de 26/05/2017 – uma vez que a contratada poderá compartilhar os recursos humanos e materiais disponíveis para execução simultânea de outros contratos – embora para a execução de determinados itens do serviço seja exigida a Presencialidade do executor ,o atendimento aos requisitos de adequada capacitação profissional, entre outros. A prestação dos serviços não gera vínculo empregatício entre os empregados da contratada e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

8.3. FORMA DE SELEÇÃO/CRITÉRIO DE JULGAMENTO DA PROPOSTA

- Considerando a natureza dos serviços e o disposto no § único do art. 25 da IN SGD/ME n°94 de 23 de dezembro de 2022,, a licitação será realizada na modalidade PREGÃO, sob a forma ELETRÔNICA, tendo como critério de julgamento, menor preço (Valor nominal, literal, expresso) para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços de informática. A fundamentação pauta-se na premissa que a contratação de serviços se baseia em padrões de desempenho e qualidade claramente definidos no Termo de Referência, havendo diversos fornecedores capazes de prestá-los, caracterizando-se como “serviço comum” conforme Art. 9º, §2º do Decreto 7.174/2010.
- O modo de disputa deverá ser ABERTO com lances decrescentes respeitando o descrito na Lei 14.133, de 2021 em seu artigo 56, § 3º.

8.4. JUSTIFICATIVA PARA A APLICAÇÃO DO DIREITO DE PREFERÊNCIA E MARGENS DE PREFERÊNCIA

- Não se aplica o disposto no art. 6º do Decreto nº 8.538/2015, que regulamenta a LC nº 123/2006, para fins de exclusividade de participação de microempresas e empresas de pequeno porte, tendo em vista que o valor previsto para a presente licitação excede o valor estipulado no decreto supra.
- No tocante aos critérios de desempate previstos na LC nº 123/2006, regulamentada pelo Decreto nº 8.538/2015, estes serão observados e disciplinados no edital.
- Em atenção ao Acórdão 1352/2018 – TCU – Plenário, que orienta aos órgãos integrantes do Sistema de Serviços Gerais (Sisg), quando da contratação de serviços de tecnologia da informação associados ao fornecimento ou locação de bens, que devem ser aplicadas as regras de preferência dispostas no Decreto nº 7.174, de 12 de maio de 2010, tais critérios serão observados e disciplinados no edital.

8.6. CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA PARA A HABILITAÇÃO

- Todas as especificações técnicas da solução de TIC descritas no termo de referência e no Anexo – Especificação Técnica da Solução de TI devem ser comprovadas mediante documentação do próprio fabricante e deverá ser inclusa em anexo na proposta de preço indicando a página e parágrafo ou captura de tela de comprovação de cada um dos subitens dos requisitos técnicos para que a empresa licitante seja habilitada.
- As empresas deverão comprovar a aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, nos termos definidos a seguir:
    - Atestado de capacidade técnica-operacional ou a Declaração emitida pelo fabricante do equipamento, comprovando que a licitante é apta a instalar, configurar, prestar garantia/manutenção e ministrar treinamentos da solução de TIC como um todo. Além disso, considerando que além da declaração específica do fabricante atestando que a licitante é distribuidora ou revenda autorizada a comercializar os itens da contratação, também é possível apresentar outra forma de comprovação, tais como contratos de adesão que autorizem a venda ou a transferência dos direitos de uso ((TCU-Acórdão/Plenário nº 3031/2008).
    - Atestado de capacidade técnica-operacional, em nome da licitante, expedido por pessoa jurídica de direito público ou privado, que comprovem a execução de no mínimo 36 meses, em contrato único ou separado, serviços de solução de segurança de perímetro NGFW contemplando o hardware, software, licenciamento, implantação, configuração, treinamento, garantia, atualizações e suporte técnico, solução de armazenamento de logs e relatoria, solução de gerenciamento centralizado de equipamentos, plataforma de ZTNA, similar à solução ofertada. Por solução similar, entende-se por solução do mesmo fabricante equipamentos com características similares ao da contratação em questão.
    - Declaração de que possuirá durante a vigência do contrato, 02 (dois) profissionais com a certificação de Engenheiro da solução de Firewall ou superior.
    - Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

- A empresa licitante deverá apresentar atestado(s) que comprove, no mínimo, atendimento à 50% dos quantitativos previstos para o item 01, e que tenha pelo menos, 50% das especificações de throughput do mesmo item, envolvendo suporte, garantia e manutenção.
- A licitante deverá comprovar experiência mínima de 3 (três) anos nas soluções de Next Generation Firewall, podendo ser aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade do período de três anos ser ininterrupto.
- A habilitação técnica será feita por intermédio de atestados ou declaração de capacidade técnica.
- Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido pelo menos um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior.
- Apresentar a composição de cada item do escopo de fornecimento, contendo marca, modelo, códigos, descritivo dos códigos, unidade, quantidades do conjunto, tudo com o objetivo de identificar claramente quais os produtos e serviços estão sendo ofertados.
- Apresentar documentação técnica (manuais e/ou catálogos do fabricante, em mídia eletrônica ou URL) comprovando o pleno atendimento de todos os requisitos técnicos, por meio de apresentação de uma planilha ponto a ponto, com indicação de nome do documento e página que comprova o atendimento.

Entende-se, para fins deste Termo de Referência, como pertencente ao quadro permanente do licitante, na data prevista para entrega da proposta, o sócio que comprove seu vínculo por intermédio de contrato/estatuto social; o administrador ou o diretor; o empregado devidamente registrado em Carteira de Trabalho e Previdência Social; e o prestador de serviços com contrato escrito firmado com o licitante, ou com declaração de compromisso de vinculação futura, caso o licitante se sagre vencedor do certame.

- É facultada a instauração de diligência destinada a esclarecer ou a confirmar a veracidade das informações prestadas pela licitante constantes de sua Comprovação de Capacidade Técnica, Proposta de Preços e de eventuais documentos anexados.
- A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MPDG n. 5 /2017.

Por fim, A licitante será considerada tecnicamente habilitada se restar inequivocamente comprovado atender integralmente ao disposto nos critérios técnicos de habilitação, dessa forma:

1. Tenha apresentado proposta de preços em conformidade com o atendimento dos requisitos estabelecidos no item 8.9.
2. Tenha apresentado Declaração de realização de vistoria técnica caso tenha a feito.
3. Tenha comprovado sua capacidade técnico-operacional através da apresentação de Atestados de capacidade técnica que atendam aos requisitos estabelecidos no item 8.6.

8.7. QUALIFICAÇÃO ECONÔMICA-FINANCEIRA

- Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput,
- inciso II).
- Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:
  - Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);
  - 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.
  - 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;
- 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.
- 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).
- O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.
- 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).

8.8. HABILITAÇÃO FISCAL, SOCIAL E TRABALHISTA

- Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ;
- 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.
- Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
- 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;
- Prova de inscrição no cadastro de contribuintes Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- Prova de regularidade com a Fazenda Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
- Caso o fornecedor seja considerado isento dos tributos 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.
- 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.

8.9. PROPOSTA

- A proposta de preços não deverá ter prazo de validade inferior a 60 (sessenta) dias corridos, a partir da data da sessão pública.
- A licitante classificada e habilitada provisoriamente em primeiro lugar para fins de comprovação de atendimento das especificações técnicas, deverá entregar em sua proposta a descrição da marca e modelo dos bens ofertados bem como toda a documentação necessária para comprovação dos requisitos que trata o anexo-Especificação Técnica da Solução de TI.
- A licitante deverá declarar, no momento de sua proposta, que possui capacidade técnica adequada para executar o objeto da licitação, atendendo aos critérios de qualidade e aos níveis de serviço exigidos, e também cumprindo os requisitos especificados para a presente contratação.
- Nos preços cotados deverão estar incluídas todas as despesas direta e indiretamente envolvidas na execução dos serviços, tais como transporte, seguros, salários, encargos sociais, encargos fiscais e taxas comerciais, impostos, taxas de contribuição, tarifas públicas e quaisquer outros custos, quando aplicáveis, necessários ao integral cumprimento do objeto contratado. Deverão estar contidos ainda todos os custos marginais referentes aos profissionais designados para a prestação dos serviços, tais como deslocamentos, hospedagens, treinamentos etc.
- A proposta deverá ser redigida em Língua Portuguesa (pt-BR), salvo quanto às expressões técnicas de uso corrente, sem emendas, rasuras ou entrelinhas, devidamente datada, sendo clara e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado, com todos os preços expressos em REAIS (R$) e declaração expressa de que os serviços ofertados atendem aos requisitos técnicos especificados no termo de referência.
- Se houver indícios de que as propostas de preços apresentadas pelas Licitantes tornem o contrato inexequível em todas ou em parte das exigências de cumprimento de obrigações contratuais, ou em caso da necessidade de esclarecimentos complementares, caberá à contratante, ao longo do processo licitatório ou a qualquer tempo, solicitar às mesmas Licitantes a demonstração de exequibilidade do contrato. Estas deverão apresentar justificativas e comprovações em relação aos custos do projeto, embasando, portanto, a decisão do MAPA a respeito da desclassificação da proposta. Caso a demonstração da exequibilidade seja insuficiente, o MAPA poderá adotar os procedimentos previstos no Anexo II da IN Nº 05/2017 - SLTI/MPDG.
- A comprovação da capacidade de atendimento a este percentual representa o mínimo razoável e compatível, em quantidades e características, para demonstrar a capacidade técnica do futuro fornecedor em prestar a integralidade dos serviços, de forma simultânea, assegurando a quantidade necessária de recursos e pessoas qualificadas para atendimento ao volume previsto nesta contratação, com garantia da qualidade e dos níveis mínimos de serviço desejados, nos termos dos incisos I e II, art. 67 da Lei nº 14.133, sendo permitido o somatório de atestados, conforme já exposto.
- Descrever individualmente e com clareza a marca, o modelo, Part Numbers, as quantidades, os valores e outras informações aplicáveis e necessárias à perfeita caracterização de cada um dos itens ofertados, assim como de todos os seus componentes expansíveis, opcionais ou que possam oferecer variação de configuração de forma a permitir a correta identificação destes na documentação técnica apresentada, obedecidas as especificações contidas neste termo de referência e seus Anexos.
- Para a solução ofertada devem ser enviados: manuais, catálogos, folhetos, impressos ou publicações originais do fabricante, formando formulário para avaliação técnica, constando a identificação e página do documento onde se encontra descrita cada uma das funcionalidades e características técnicas descritas neste termo de referência.

8.10. PARTICIPAÇÃO DE CONSÓRCIOS E COOPERATIVAS

- É vedada a participação de empresas em consórcio ou cooperativas; qualquer que sua forma de constituição, considerando as características específicas da contratação dos serviços a serem fornecidos, que não pressupõem multiplicidade de atividades empresariais distintas para execução do objeto.

8.11. ADMISSIBILIDADE E LIMITES DA SUBCONTRATAÇÃO

É permitida a subcontratação total para a execução do objeto para os seguintes itens:

- Elaboração do projeto de implantação.
- Instalação completa da solução de TIC.
- Visitas mensais preventivas e atendimento técnico de tickets de garantia.
- Treinamento.

8.12. VERIFICAÇÃO DE AMOSTRA DO OBJETO

- A possibilidade de verificação de amostra, tem previsão no artigo 17, §3º, artigo 41, inciso II, e artigo 42, §2º, todos da Lei nº 14.133, de 2021, e no artigo 12, § 1º da IN SGD/ME nº 94, de 2022. Portanto, como são equipamentos de altos valores, o Ministério poderá solicitar amostra se assim desejar.
- Para fins de aceitação pelo MAPA, este Ministério poderá solicitar amostra para aferir as funcionalidades dos equipamentos em testes de bancada. Os itens de performance serão comprovados mediante datasheet ou declaração do fabricante em casos excepcionais. Os testes de bancada são destinados, exclusivamente, a dirimir dúvidas dos demais participantes do certamente licitatório, quando suscitadas, sobre as capacidades dos equipamentos que serão entregues pelo participante vencedor do certame. Os testes de bancadas consistirão em:
    - Aferição da capacidade de throughput de tráfego descriptografado pelo equipamento a ser testado.
    - Aferição da capacidade de trhoughput de inspeção de tráfego SSL do equipamento a ser testado.
    - Aferição das especificações técnicas (portas de comunicação, capacidade de processamento, memórias estáticas e volátil) do equipamento a ser testado.
    - Capacidades do software do equipamento a ser testado.

Os critérios mínimos de aceitação serão os seguintes:

    - Relativamente aos testes de throughput, o equipamento testado deve apresentar, no mínimo, 95% da capacidade
    - declarada, considerado o fato de que se trata de uma simulação em ambiente controlado.
    - Todas as funcionalidades de software devem corresponder às declaradas pelo fabricante em sua plenitude.

- O ambiente para realização dos testes, bem como os cenários de testes, serão providenciados pelo vencedor do certamente, e devem ser passíveis de inspeção quanto às configurações e capacidades por todos os atores envolvidos Mapa e demais licitantes interessados. O vencedor do certamente deverá assegurar que todos os interessados possam realizar a inspeção do ambiente e acompanhar os testes in-loco.
- Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos às sanções previstas em lei.
- Apresentação e avaliação da amostra seja oportunizada na fase de julgamento, podendo gerar a desclassificação do licitante provisoriamente classificado em primeiro lugar se a amostra não for apresentada no prazo ou se for reprovada nos testes de bancada.
- Para fins de comprovação de atendimento das especificações técnicas, a empresa declarada provisoriamente vencedora do certame licitatório deverá realizar a demonstração do teste de bancada em sua dependência preferencialmente em Brasília, o equipamento para ser testado no prazo de até 30 (trinta) dias corridos após a realização do processo licitatório.

    - Caso os testes não sejam realizados em Brasília, cabe a empresa provisoriamente classificada em primeiro lugar, arcar com as despesas de viagem do time de avaliação do MAPA.
- Estes testes visam verificar se o produto ofertado atende às especificações requeridas no ambiente de produção real.
- A proponente classificada deverá indicar na sua proposta comercial, após o final da disputa de lances, a composição da sua equipe técnica. Tal equipe será a responsável pela realização do teste de conformidade e deverá ser composta por até 5 (cinco) técnicos ou representantes legais da proponente, do fabricante da solução ou de empresa especializada na realização de testes de bancada. As demais licitantes participantes do pregão poderão acompanhar os testes de bancada. Para isso, deverão informar previamente ao MAPA, indicando até 2 (dois) técnicos ou representantes legais (seus ou do fabricante da solução), sendo de sua responsabilidade acompanhar os prazos e datas junto ao MAPA.
- Não será permitida a substituição de qualquer dos componentes da equipe técnica da proponente convocada ou da equipe técnica de acompanhamento sem a autorização prévia do MAPA. O Firewall, gerenciamento e demais equipamentos necessários à execução do teste de bancada deverão ser instalados, configurados, operados e acessados pela Equipe Técnica da licitante convocada/subcontratada, sempre acompanhada e supervisionada por servidores de tecnologia da informação do MAPA.

- Para qualquer dúvida que surja deverá ser utilizada a especificação do edital e termo de referência para dirimi-la. A não observância do item acima poderá acarretar no reinício do Teste de Bancada, sem concessão de prazo adicional, ou mesmo na reprovação da solução ofertada.
- Os testes devem ser realizados com uma unidade do firewall, não sendo permitido utilizar duas caixas. Se a equipe técnica da proponente não conseguir ativar alguma funcionalidade solicitada durante os testes de bancada, o equipamento será considerado reprovado.
- Todo e qualquer custo de equipamento, software e equipe técnica disponibilizados para a realização dos testes é de responsabilidade da proponente.
- O conceito de amostra para o referido teste é o conjunto que consiste em um firewall NGFW de modelo igual ao da solução de alta disponibilidade ofertada, mais a solução de gerenciamento centralizado que compõe a solução, com todos os módulos licenciados e habilitados.
- A proponente deve prover, além da amostra, toda a infraestrutura necessária (equipamentos e cabos de conectividade de rede, equipamentos de geração de tráfego e ameaças, appliances, servidores de virtualização, desktops, todos os softwares e licenças de utilização e demais acessórios) para a completa instalação e execução do teste de bancada.
- Todos os equipamentos e produtos que compõem a amostra da solução ofertada deverão estar acompanhados de seus respectivos programas, CDs, manuais, guias de instalação e demais documentos necessários para dirimir dúvidas, a fim de que possam ser realizados procedimentos de verificação de conformidade com as especificações técnicas constantes do edital. O conjunto de equipamentos especializados de geração de tráfego e ameaças deve ser capaz de simular pelo menos 100 aplicações.
- A licitante convocada deverá fornecer, em meio eletrônico ou digital, juntamente com a proposta comercial e a documentação obrigatória, a relação de ameaças (ataques, vírus, malwares, etc.) e aplicações (Skype, TeamViewer, BitTorrent, etc.) que podem ser detectados pela solução ofertada, em sua versão mais atualizada, incluindo suas classificações de severidade e de precisão e esforço de detecção.
- Preparação inicial, a ser realizada no início da fase de execução:
    - A amostra deve ser inicialmente submetida a procedimento de “factory reset”, “factory default” ou equivalente. A amostra deve então ser atualizada para a versão mais atual de firmware, software, listas de assinaturas e afins disponíveis pelos canais oficiais de suporte técnico do fabricante da solução. Caso a versão do sistema operacional atual tenha menos de 4 (quatro) meses de liberação de uso para o mercado, será admitida a utilização da versão imediatamente anterior.
    - Deverão ser aplicadas todas as correções, patches, fixes e afins recomendados pelo fabricante da solução em seus canais oficiais de suporte técnico. Não serão aceitas versões, correções ou afins em estágios de testes (versões alfa e beta, release candidates, early availability, etc.).
- Não serão aceitas correções, patches, fixes e afins que não tenham previsão de serem incorporados em futuras versões do firmware ou software da solução ofertada.
- O firewall e demais equipamentos devem ser instalados e configurados de forma a simular uma arquitetura de rede.

9. Estimativas do Valor da Contratação

Valor (R$): 6.283.761,68

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

ITEM	ESPECIFICAÇÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
01	Firewall - Solução de plataforma de segurança denominada Next Generation Firewall (NGFW) com instalação, suporte, garantia e licenciamento inclusos.	04 unidades	R$ 1.306.986,00	R$ 5.227.944,00
02	Solução de armazenamento de logs e relatoria, com instalação, suporte, garantia e licenciamento inclusos	01 unidade	R$ 126.480,86	R$ 126.480,86
03	Solução para gerenciamento centralizado dos equipamentos, com instalação, suporte, garantia e licenciamento inclusos.	01 unidade	R$ 103.007,54	R$ 103.007,54
04	Treinamento ministrado por profissional certificado pelo fabricante.	01 unidade	R$ 43.662,61	R$ 43.662,61

05	Plataforma de ZTNA - Zero Trust Network Access, com instalação, suporte, garantia e licenciamento inclusos.	01 unidade	R$ 782.666,67	R$ 782.666,67

10. Adequação orçamentária

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. - As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.
10.2 - A contratação será atendida pela seguinte dotação:

- Programa de Governo: 0032 - Programa de Gestão e Manutenção do Poder Executivo Federal.
- Ação Orçamentária: 2000 - Administração da Unidade
- Plano Orçamentário: 0009 - Gestão e Manutenção de Soluções e Processos de Tecnologia da Informação
- Fonte Orçamentária: 100
- Plano Interno: PROGESTÃO

10.3 - Cronograma Físico Financeiro
A seguir, estima-se o cronograma de execução Físico-Financeira:

GRUPO	ITEM	ESPECIFICAÇÃO	QTDE	1º ANO	2 º ANO	3 º ANO	4 º ANO	5º ANO
ÚNICO	01	Firewall - Solução de plataforma de segurança denominada Next Generation Firewall (NGFW) com instalação, suporte, garantia e licenciamento inclusos.	04 unidades	R$ 5.227.944,00	-	-	-	-
	02	Solução de armazenamento de logs e relatoria, com instalação, suporte, garantia e licenciamento inclusos.	01 unidade	R$ 126.478,78	-	-	-	-
	03	Solução para gerenciamento centralizado dos equipamentos, com instalação, suporte, garantia e licenciamento inclusos.	01 unidade	R$ 103.006,04	-	-	-	-
	04	Treinamento ministrado por profissional certificado pelo fabricante.	01 unidade	R$ 43.662,61	-	-	-	-
	05	Plataforma de ZTNA - Zero Trust Network Access, com instalação, suporte, garantia e licenciamento inclusos.	01 unidade	R$ 782.666,67	-	-	-	-
TOTAL ESTIMADO				R$ 6.283.761,68				
Os pagamentos serão conforme os requisitos temporais, recebimento do objeto e critérios de aceitação de bens fornecidos, tópicos estes discriminados ao longo do termo de referência. Não há como determinar com exatidão as datas acima.								

11. Reajuste Contratual.

11.1 - Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 20.12.2023.
11.2 - Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na fórmula es pulada pelo Art. 5º do Decreto nº 1.054, de 7 de fevereiro de 1994:

R = V x I – Io,
onde: R = Valor do reajuste procurado.
V = Valor contratual do serviço a ser reajustado.
I = Índice relativo à data do reajuste.
Io = Índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta na licitação.

11.3 - Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.
11.4 - Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.
11.5 - Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.
11.6 - Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

12. Garantia Contratual

12.1. - O adjudicatário, no prazo de 10 (dez) dias após a assinatura do termo de contrato, prestará garantia no valor correspondente a 6,5% (seis e meio por cento) do valor global do contrato, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 100 da Lei Nº 14.133 de 2021, desde que cumpridas as obrigações contratuais.
12.2. - O CONTRATADO apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do contratante, contado da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública ou, ainda, pela fiança bancária, em valor correspondente a 6,5% (seis e meio por cento) do valor anual do contrato.
12.3. - A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autoriza o MAPA a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme disposto na Lei nº 14.133.
12.4. - A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual, conforme item 3.1 do Anexo VII-F da IN SEGES/MPDG nº 5/2017. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:
a) Prejuízos advindos do não cumprimento do objeto do contrato ou multas;
b) Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato; Multas moratórias e punitivas aplicadas pela Administração à contratada.
12.5. - A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria. O garantidor não é parte legítima para figurar em processo administrativo instaurado pelo MAPA com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada (cfe. IN nº 05/2017).
12.6. - A garantia em dinheiro deverá ser efetuada em favor do MAPA. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo MAPA, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.
12.7. - No caso de alteração do valor do contrato ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a contratada obriga-se a fazer a respectiva reposição no prazo máximo de 05 (cinco) dias úteis, contados da data em que for notificada.
12.8. - O MAPA executará a garantia na forma prevista na legislação que rege a matéria. Será considerada extinta a garantia:
a) Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a

título de garantia, acompanhada de declaração do MAPA, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato;
b) No prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h" do item 3.1 do Anexo VII-F da IN SEGES/MP n° 05/2017.
12.9. A contratada autoriza o MAPA a reter, a qualquer tempo, a garantia, na forma prevista neste termo de referência e no contrato.

13. Equipe de Planejamento da contratação

13.1. - A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 18, de 28 de março de 2023 CGAQ/MAPA (SEI Nº 27579550).
13.2. - Certificamos que as diretrizes estabelecidas no termo de referência são as adequadas ao atendimento do interesse público envolvido, estando compatíveis com o estudo técnico preliminar da contratação. Além disso, o instrumento contém todos os elementos necessários para a caracterização da contratação. Além disso, certificamos, ainda, que as especificações técnicas previstas neste Termo de Referência atendem às premissas contidas na IN SGD/ME Nº 04, de 23 de Dezembro de 2022.
13.4. - Por fim, conforme o §6º do art. 12 da IN SGD/ME Nº 94 de 2022, o Termo de Referência será assinado pela Equipe de Planejamento da Contratação, pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

14. 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.

THIAGO PEREIRA DA COSTA
Membro da comissão de contratação
Assinou eletronicamente em 13/03/2024 às 16:22:14.

MARCO ANTONIO BITTENCOURT SUCUPIRA
Membro da comissão de contratação
Assinou eletronicamente em 13/03/2024 às 17:13:04.

CARLA CRISTIANE DE ABREU OLIVEIRA
Membro da comissão de contratação
Assinou eletronicamente em 14/03/2024 às 14:31:03.

CAMILO MUSSI

Autoridade competente

Assinou eletronicamente em 13/03/2024 às 17:26:23.

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 - Anexo - Especificacao Tecnica da Solucao de TI.pdf (208.77 KB)
- Anexo II - Anexo-Vistoria.pdf (15.86 KB)
- Anexo III - Ordem de Servico.pdf (177.26 KB)
- Anexo IV - Termo de Ciencia.pdf (178.08 KB)
- Anexo V - Termo de Compromisso de Manutencao de Sigilo.pdf (237.01 KB)
- Anexo VI - Termo de Recebimento Definitivo.pdf (204.9 KB)
- Anexo VII - Termo de Recebimento Provisorio.pdf (183.45 KB)

Anexo I - Anexo - Especificacao Tecnica da Solucao de TI.pdf

ITEM 1 – 04 equipamentos denominados Next Generation Firewall (NGFW).

FUNCIONALIDADES DE FIREWALL

- A solução deve consistir em appliances de proteção de rede com funcionalidades de proteção de próxima geração.
  - As funcionalidades de proteção de rede que compõem a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica.
  - O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.
- A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede.
  - Realizar upgrade via https via interface WEB.
  - Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
    - Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames.
    - Deverá suportar VXLAN.
  - Deve suportar os seguintes tipos de NAT:
    - Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente. ◦ Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.
    - As regras de NAT devem suportar "hit count" para monitorar a quantidade de conexões que deram matches em cada regra.
    - Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizáveis de forma dinâmica, por exemplo: Office 365, AWS e outros. Objetos dinâmicos que não se caracterizam como FQDN.
  - Enviar logs para sistemas de monitoração externos, simultaneamente.
  - Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção.
  - Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall.
  - Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).
  - Suportar OSPF graceful restart.
  - Deve suportar roteamento ECMP (equal cost multi-path).
  - Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultânea usando os seguintes parâmetros: Origem, Destino, Porta de Origem, Porta de Destino e Protocolo.
  - Autenticação integrada via Kerberos.
  - A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problemas. Entre as funções, deve suportar no mínimo: acesso SSH, SCP, acesso WEB, alterações de política, comunicação SNMP.
  - As regras Firewall devem suportar "hit count" para monitorar a quantidade de conexões que deram matches em cada regra.
  - Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas.
  - A solução deve ter a capacidade de operar através de uma única instância de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer

(monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3).

- A solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos.
- Deve possuir mecanismo de ativação de validade da regra com período customizado.
- Deverá suportar redundância e balanceamento de links, tendo capacidade de no mínimo 3 links de internet. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.
- Deve permitir a configuração do tempo de checagem para cada um dos links.

CONTROLE DE APLICAÇÕES

- Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações.

- Controle de políticas por usuários, grupos de usuários, IPs e redes.
- Deve descriptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3.
- Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
- Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos.
- Reconhecer aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.
- A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não.
- Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE).
- Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas.
- Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo.
- A fim de otimização do tempo operacional dos administradores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante.
- Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.).
- Possui mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação principal e/ou as suas sub-categorias. Quando o administrador da solução desejar bloquear apenas as sub-categorias do facebook, como facebook, chat, video, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como “Facebook” ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter, YouTube, etc. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote.
- A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação.
- Atualizar a base de assinaturas de aplicações automaticamente e Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.
- Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários

do sistema do Active Directory.

- Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística.
- Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão.
- Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.
- A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
  - Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).
  - Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes. ◦ Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via Active Directory e base de dados local.

◦ Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.
◦ Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs.
◦ Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário. ◦ Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs.
◦ Suportar a criação de categorias de URLs customizadas e a exclusão de URLs do bloqueio, por categoria.
◦ Permitir a customização de página de bloqueio.
◦ Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede.
◦ Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários.
◦ Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal). O uso de Captive Portal deve poder ser configurado para ser obrigatório ou não.

PREVENÇÃO CONTRA AMEAÇAS

- Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall.

- Possuir capacidade de detecção de assinaturas de ataques pré-definidos.

- Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo.
- Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
- A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo.
- Deverá possuir os seguintes mecanismos de inspeção de IPS:
  - Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e

bloqueio de pacotes malformados.
  - ◦ Detectar e bloquear a origem de portscans.
  - ◦ Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações.
  - ◦ Possuir assinaturas para bloqueio de ataques de buffer overflow.
  - ◦ Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP.
  - ◦ Suportar bloqueio de arquivos por tipo.
  - ◦ Identificar e bloquear comunicação com botnets.
  - ◦ Deve suportar referência cruzada com CVE.
- ● Em cada proteção de segurança, deve estar incluso informações como:
  - ◦ Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro código de referência.
  - ◦ Severidade.
  - ◦ Tipo de ação a ser executada.
- ● O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.
- ● O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.
- ● O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.
- ● O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor).
- ● Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: ◦ O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção.
- ● Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada.
- ● Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual.
- ● A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção deve ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.
- ● A solução deverá possuir pelo menos dois perfis pré configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado.
- ● A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.
- ● Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms.
- ● Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados.
- ● O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento.
- ● A solução de IPS deve possuir engine onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual.
- ● O antivírus deve oferecer suporte à verificação de links dentro de e-mails.
- ● A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso.
- ● A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada.

- Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente.
- A solução deve permitir a criação de White list baseado no MD5 do arquivo.
- Os eventos devem identificar o país de onde partiu a ameaça.
- A funcionalidade de IPS e anti-bot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de técnicas de acordo com a ameaça detecada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas.
- Suportar rastreamento de vírus em arquivos pdf.
- Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.).
- Em caso de falha no mecanismo de inspeção do Anti-Vírus, deve ser possível configurar se as conexões serão permitidas ou bloqueada.
- A solução de Antivírus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day).
- A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede.
- Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado.
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
- Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.
- A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.
- A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & Control).
- A solução Antivírus deverá suportar a análise de links no corpo de emails.

FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

- Objetivando controlar aplicações e tráfego cujo consumo possa impactar o desempenho de rede, como streaming de mídias, a solução, além de permitir ou negar esse tipo de aplicação, deve ter a capacidade de limitá-las por políticas de controle de taxa de transmissão, quando solicitadas por diferentes usuários ou aplicações, tanto de streaming de áudio como de vídeo.
- Suportar a criação de políticas de QoS por Endereço de origem, Endereço de destino, Por usuário e grupo do LDAP/AD, Por porta; e Por tipo de tráfego.
- As funcionalidades de QoS e Traffic Shaping devem possibilitar a definição de classes por: Banda garantida, Banda máxima por usuário, Banda máxima por aplicação e Fila de prioridade.
- Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP, dentre outros.
- Suportar marcação de pacotes diffserv.
- Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

FILTRO DE DADOS

- Permitir a criação de filtros para arquivos e dados pré-definidos.
- Os arquivos devem ser identificados por extensão e assinaturas.

- Suportar a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.
- Permitir listar o número de aplicações suportadas para controle de dados e Permitir listar o número de tipos de arquivos suportados para controle de dados.

ALTA DISPONIBILIDADE E BALANCEAMENTO DE CARGA

- Permitir a configuração dos appliances em modo de alta disponibilidade, com suporte mínimo aos seguintes modos de configuração: Ativo-Ativo.
- A alternância entre os dispositivos configurados em modo de alta disponibilidade deve se dar no mínimo pelos seguintes parâmetros de detecção de anomalia:
  - Falha de funcionamento do dispositivo.
  - Falha de link, seja por falha no tráfego (path monitoring) quanto por falha no tráfego das suas interfaces (Interface Monitoring).
- Deverá ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino, que deverá estar comunicável através da rota. Caso haja falha na comunicação, o firewall deverá ter a capacidade de usar alternativa para restabelecer a comunicação.
- Operando em alta disponibilidade, os dispositivos deverão, no mínimo, sincronizar as seguintes informações entre si:
  - Certificados digitais, informações registradas em sua Forwarding Information Base(FIB), configurações registradas em suas políticas de firewall incluindo em seus objetos de rede, configurações de NAT e possuir administração através de linha de comando através de SSH versão 2 e através de interface WEB.
- A solução de balanceamento deve possuir a capacidade de, automaticamente, por meio de definições de thresholds, executar a realocação de equipamentos entre os clusters, ou o redirecionamento do tráfego sem a necessidade de intervenção física para este redirecionamento.

DETECÇÃO E TRATAMENTO POR MALWARES DESCONHECIDOS

- Ser capaz de detectar e analisar malwares desconhecidos, ou seja, que não estejam na base de registro de assinaturas da solução, utilizando-se para tal de recursos avançados, como o uso de sandbox para isolamento e tratamento de ameaças.
- Monitorar os arquivos trafegados na internet em protocolos HTTP, HTTPS e SMTP.
- Monitorar os arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e Layer 3.
- Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.
- A análise de malwares não conhecidos em ambiente controlado (sandbox) também deve ser realizada em arquivos tipo executáveis, DLLs,arquivos compactados RAR, .zip e 7-ZIP, arquivos do pacote MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos PDF, arquivos JAVA (.jar e class), arquivos DMG,arquivos ELF e arquivos APK.
- Ser capaz de detectar e analisar arquivos suspeitos em ambiente Sandbox simulando, no mínimo, os sistemas operacionais Windows 10 e superiores e Microsoft Office.
- Realizar o envio automático de arquivos trafegados na rede MAPA para análise Sandbox, onde o arquivo será executado e simulado em ambiente controlado.
- Permitir o envio para análise em Sandbox de malwares bloqueados pelo antivírus da solução.
- A seleção dos arquivos para envio para análise deverá se dar por meio políticas granulares de segurança, considerando-se parâmetros próprios da solução Firewall NGFW, como endereço IP de origem/destino, usuário/grupo de usuários, aplicação, protocolo/porta, URL e categoria de URL, tipo de arquivo.
- Diferenciar os arquivos analisados em pelo menos três categorias:

    - Malicioso.
    - Não maliciosos.
    - Não maliciosos, mas com características indesejáveis.
    - Entende-se como "não malicioso, mas com características indesejáveis"; softwares que causem problemas de performance em dispositivos, tais como lentidão na execução do sistema operacional, ou que alterem parâmetros de sistema, como alterações no registro do Windows.
- Suportar a análise Sandbox de arquivos executáveis, DLLs, compactados (.zip, .rar, .7-zip etc.) e criptografados em tráfego SSL.
- Suportar a análise Sandbox de arquivos do pacote Microsoft Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e .class), e arquivos do sistema operacional Android.
- Capacidade de análise de links em Sandbox, com registro posterior na base de filtro de URL da solução, caso o link analisado em Sandbox for classificado em categorias maliciosas, como "phishing".
- Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.
- Permitir exportar, a partir da própria console de gerenciamento da solução, o resultado das análises de malwares do tipo "Zero Day" em arquivo tabulado, como .txt; .csv ou .pdf.

SEGURANÇA EM TRÁFEGO CRIPTOGRAFADO

- O controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e de saída (Outbound);
- O "offload" de certificado em inspeção de conexões SSL de entrada (Inbound).
- Descriptografar o tráfego Inbound e Outbound em conexões negociadas com TLS v 1.3 ou superior.
- Inspeção e de-criptografia de SSH com base em políticas de segurança.
- Deverá possibilitar a identificação e o bloqueio de tráfego, caso o protocolo esteja sendo usado como técnica evasiva para burlar os controles de segurança;
- Descriptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
- Deverá permitir o espelhamento de tráfego descriptografado (SSL e TLS) para análise por meio de soluções externas de segurança, por exemplo, soluções de análise forense de rede, ferramentas de auditoria, Data Loss Prevention, etc.

SEGMENTAÇÃO E ENDEREÇAMENTO DE REDE

- Cada dispositivo Firewall NGFW, deve permitir as seguintes configurações mínimas de segmentação e endereçamento de rede:
    - Deverá suportar controles por zona de segurança.
    - Suporte a pelo menos 10 (dez) roteadores virtuais.
    - Permitir a criação de sub-interfaces lógicas Ethernet.
    - Suportar a criação de pelo menos 150 VLANs (802.1q tags) por dispositivo e por interface.
- Suportar agregação de links por meio de implementação 802.3ad Link Aggregation e Link Aggregation Control Protocol (LACP).
- Permitir configuração de balanceamento de link através de, no mínimo, uma das seguintes opções:
    - Por políticas aplicadas a usuário ou grupos de usuários do LDAP/Active Directory ou
    - Por políticas configuradas por aplicação e porta de destino.
- Permitir a configuração de interfaces nos seguintes modos:
    - Sniffer: Monitoramento e análise de tráfego por espelhamento de porta local (SPAN) ou remota (RSPAN).
    - Layer 2 switching, com ou sem utilização de VLAN's.
    - Layer 3 routing.

○ Modo transparente ou “virtual wire” (interconexão de portas do Firewall NGFW). ○ Agrupamento de interfaces (IEEE 802.1AX link aggregation).
○ Misto: Mais de um modo de configuração de interface no mesmo appliance.

- Permitir o roteamento ou encaminhamento de pacotes baseado em políticas (PBF - Policy Based Forwarding).
- Implementar recursos de Network Address Translation (NAT) em redes IPv4 e IPv6, incluindo implementação em rede híbrida (NAT64), com suporte mínimo aos seguintes recursos:
  ○ NAT de Origem e de NAT de Destino, configurados isolada ou simultaneamente.
  ○ NAT estático do tipo “One-to-One”, bidirecional “One-to-One” e “Many-to-Many”.
  ○ NAT dinâmico do tipo “Many-to-One” e “Many-to-Many”.
  ○ NAT Overload com tradução de endereço de porta (PAT).
  ○ NAT para interfaces conectadas virtualmente (Virtual Wire), com implementações mínimas de NAT Estático, NAT de Origem e NAT de Destino.

VPN

- Suportar VPN Site-to-Site.
- Suportar IPSEC VPN.
- A VPN IPSEC deve suportar:
  - 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI.
- Suportar SSL VPN o qual deve:
  - Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.
- Suportar autenticação via AD/LDAP, certificado e base de usuários local.
- Suportar leitura e verificação de CRL (certificate revocation list).
- O agente de VPN SSL client-to-site deve ser compatível com pelo menos:
  - Windows, Linux e Mac OS X.
- Deve suportar duplo fator de autenticação para a conexão VPN.
- Capacidade para, no mínimo, 500 conexões simultâneas.

SEGURANÇA DE DNS

A solução deve mostrar nos logs as seguintes informações sobre domínios DGA (Domain Generation Algorithm):

- Domínio suspeito identificado;
- ID de assinatura de detecção;
- Usuário logado na estação/servidor que originou o tráfego;
- Aplicação;
- Porta de destino;
- IP de origem;
- Horário;
- Ação do firewall;
- Severidade;
- A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle.

PREVENÇÃO DE AMEAÇAS AVANÇADAS (ZERO DAY)

- O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado.
- Deve ser capaz de enviar para análise, arquivos tipo Executáveis, DLLs, Arquivos de Código e MSI.
- A solução deve detectar e bloquear em tempo real (inline) os artefatos maliciosos desconhecidos (zero day) no próprio GW através de mecanismos de Machine Learning.
- Suportar a análise dinâmica de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows 10, Mac OS X, Android, Linux.
- A análise de links em sandbox deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução.
- Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência.
- Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.
- Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante.
- Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado.
- Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox.
- As funcionalidades de sandbox tem como objetivo, analisar e bloquear em tempo real de Ameaças Avançadas Persistentes - APT. Essas funcionalidades têm o objetivo de proteger o ambiente contra a entrada de malwares não conhecidos, e para que ela seja efetiva é necessário que a inspeção e bloqueio sejam feitas em linha (inline), através de features de machine learning.
- Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.
- A solução deve analisar os arquivos do tipo malware em bare metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.
- Deve prevenir contra-ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript.
- Deve ser capaz de aplicar de forma complementar às assinaturas de antivirus a inspeção inline através de Machine learning em tempo real arquivos tipo PE (portable executable), ELF (executable and linked format) e Arquivos Microsoft Office, bem como, scripts PowerShell e shell script em tempo real para malwares desconhecidos.

ITEM 05 (Zero Trust Network Access)

Deverá ter a característica de Zero Trust Network Access e funcionalidades para no mínimo **400** usuários simultâneos com os seguintes aspectos:

- Deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas.
- Deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão.
- Deve prover um método para controlar o acesso, identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust.

- A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário.
- Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem.
- O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante.
- Deve ser compatível com pelo menos os seguintes sistemas operacionais: Windows e Linux.
- Deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.2 e 1.3. Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários.
- A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso.
- Deve ser possível revogar o certificado de um agente por meio da console central.
- O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso.
- No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão.
- Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional.
- A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até 05 dias anteriores ao ocorrido.
- Deve existir a possibilidade de restringir o usuário de realizar backup da configuração do agente.
- Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes.
- A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4. Deve ser possível agrupar agentes em grupos e atribuir grupos de agentes a perfis de políticas específicas.
- Deve ser possível exigir uma senha para desconectar o agente da console central.
- Deve ser possível evitar que o usuário realize shutdown do agente após estar registrado na console central. A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA.
- Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas.
- A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa.

- Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais. Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente que não esteja em conformidade possa se conectar a redes críticas.
- A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional. Além disso, deve ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows.
- Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar.

Anexo II - Anexo-Vistoria.pdf

ANEXO- MODELO DE DECLARAÇÃO DE REALIZAÇÃO DA VISTORIA TÉCNICA OU OPÇÃO POR NÃO REALIZAÇÃO

DECLARAÇÃO DE REALIZAÇÃO DA VISTORIA TÉCNICA

DECLARAMOS, para fins de participação no Pregão Eletrônico n° ____/2023, que a empresa <Razão Social da Empresa>, registrada no CNPJ/MF <CNPJ>, representada por seu Responsável Técnico abaixo identificado, realizou VISTORIA TÉCNICA nas instalações da Coordenação-Geral de Infraestrutura, Cibersegurança e Serviços de TI da Subsecretaria de Tecnologia da Informação do Ministério da Agricultura e Pecuária, tomando ciência de informações e instruções necessárias ao atendimento do objeto da presente licitação e à eventual elaboração de sua PROPOSTA.

Data
Nome
Cargo
Assinatura

DECLARAÇÃO DE NÃO REALIZAÇÃO DA VISTORIA TÉCNICA

DECLARAMOS, para fins de participação no Pregão Eletrônico n° ____/2023, que a empresa <Razão Social da Empresa>, registrada no CNPJ/MF <CNPJ>, em conformidade com a previsão contida no item 4.12 do Termo de Referência, manifestamos nossa opção por **não realização** da Vistoria Técnica.

Data
Nome
Cargo
Assinatura

Anexo III - Ordem de Servico.pdf

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

ORDEM DE SERVIÇO OU DE FORNECIMENTO DE BENS

INTRODUÇÃO
Por intermédio da Ordem de Serviço (OS) ou Ordem de Fornecimento de Bens (OFB) será solicitado formalmente à Contratada a prestação de serviço ou o fornecimento de bens relativos ao objeto do contrato. O encaminhamento das demandas deverá ser planejado visando a garantir que os prazos para entrega final de todos os bens e serviços estejam compreendidos dentro do prazo de vigência contratual. **Referência: Art. 32 IN SGD Nº 94/2022.**

1 – IDENTIFICAÇÃO			
Nº da OS/OFB	xxxx/aaaa	**Data de emissão**	<dd/mm/aaaa>
CONTRATO/NOTA DE EMPENHO nº	xx/aaaa		
Objeto do Contrato	<Descrição do objeto do contrato>		
Contratada	<Nome da contratada>	**CNPJ**	99.999.999/9999-99
Preposto	<Nome do preposto>		
Início vigência	<dd/mm/aaaa>	**Fim vigência**	<dd/mm/aaaa>
ÁREA REQUISITANTE			
Unidade	< Sigla – Nome da unidade>		

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Solicitante	<Nome do solicitante>	E-mail	xxxxxxxxxxxx

2 – ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES ESTIMADOS

Item	Descrição do bem ou serviço	Métrica	Valor unitário (R$)	Qtde/Vol.	Valor Total (R$)
1	...	...	...	...	...
...	...	...	...	...	...
Valor total estimado da OS/OFB					

3 – <INSTRUÇÕES/ESPECIFICAÇÕES> COMPLEMENTARES

<Incluir instruções complementares à execução da OS/OFB>

<Ex.: Contatar a área solicitante para agendamento do horário de entrega>

<Ex.: Conforme consta no Termo de Referência, o recebimento provisório está condicionado à entrega do código no ambiente de homologação, e a documentação do software no repositório oficial de gestão de projetos>

4 – DATAS E PRAZOS PREVISTOS

Data de Início:	<dd/mm/aaaa>	Data do Fim:	<dd/mm/aaaa>

CRONOGRAMA DE EXECUÇÃO/ENTREGA

Item	Tarefa/entrega	Início	Fim
1		<dd/mm/aaaa>	<dd/mm/aaaa>
...		<dd/mm/aaaa>	<dd/mm/aaaa>

5 – ARTEFATOS / PRODUTOS

Fornecidos	A serem gerados e/ou atualizados

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

5 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA

Autoriza-se a <execução dos serviços / entrega dos bens> correspondentes à presente <OS/OFB>, no período e nos quantitativos acima identificados.

_____	_____
<Nome >	<Nome >
<Responsável pela demanda/ Fiscal Requisitante>	**Gestor do Contrato**
Matr.: <Nº da matrícula>	Matr.: <Nº da matrícula>

<Local>, xx de xxxxxxxxx de xxxx

Anexo IV - Termo de Ciencia.pdf

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Histórico de Revisões

Data	Versão	Descrição	Autor
DD/MM/AAAA	1.0	Primeira versão do documento.	XXXXXXXXXXX

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

TERMO DE CIÊNCIA

INTRODUÇÃO
O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão/entidade. No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados. **Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO Nº	xxxx/aaaa		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	**CNPJ**	xxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	**MATR.**	xxxxxxxxxxxxx

2 – CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	**Matrícula**	**Assinatura**
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
…	…	…

<Local>, <dia> de <mês> de <ano>.

Anexo V - Termo de Compromisso de Manutencao de Sigilo.pdf

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Histórico de Revisões

Data	Versão	Descrição	Autor
DD/MM/AAAA	1.0	Primeira versão do documento.	XXXXXXXXXXX

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO
O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não. **Referência: Art. 18, Inciso V, alínea "a" da IN SGD/ME Nº 94/2022.**

Pelo presente instrumento o <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, doravante denominado **CONTRATANTE**, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do **CONTRATO N.º <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO,** doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

[...]

[...]

[...]

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

[...]

[...]

[...]

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

[...]

[...]

[...]

4 – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

[...]
[...]
[...]

5 – DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face

da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

[...]

[...]

[...]

6 – VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

[...]

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

[...]
[...]
[...]

8 – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

[...]
[...]
[...]

9 – FORO

A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

[...]

10 – ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	**CONTRATANTE**
_____ <Nome> <Qualificação>	_____ <Nome> **Matrícula:** xxxxxxxx
TESTEMUNHAS	
_____ <Nome> <Qualificação>	_____ <Nome> <Qualificação>

<Local>, <dia> de <mês> de <ano>.

Anexo VI - Termo de Recebimento Definitivo.pdf

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Histórico de Revisões

Data	Versão	Descrição	Autor
DD/MM/AAAA	1.0	Primeira versão do documento.	XXXXXXXXXXX

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

<Nas contratações de licenciamento de softwares, é imprescindível verificar se toda a documentação entregue pela contratada está completa e corresponde exatamente ao que foi especificado no TR. É fundamental certificar-se de que todas as licenças, suporte e/ou garantia entregues estejam de acordo com os **part numbers** especificados no TR>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO
O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelelcidos. **Referência: Inciso XXII, Art. 2º e alínea "h" inciso I do art. 33, da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OS/OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO				
SOLUÇÃO DE TIC				
<descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>				
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**	**TOTAL**
1	<descrição igual à da OS/OFB de abertura>	<Ex.: PF>	<n>	<total>
...				
TOTAL DE ITENS				

3 – ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea "h", da IN SGD/ME nº 94/2022, por este instrumento ATESTO/ATESTAMOS que o(s) <serviço(s)/ bem(s)> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela **CONTRATADA** e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDIMENTO	OBSERVAÇÃO
1	<exigência contratual estabelecida no TR >	...	.....
...	...	...	.....
...	...	...	.....
...	...	...	.....

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.

Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

5 – ASSINATURA

GESTOR DO CONTRATO

_____

<Nome do Gestor do Contrato>
Matrícula: xxxxxxxx

<Local>, <dia> de <mês> de <ano>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

<As seções seguintes podem constar em documento diverso, pois dizem respeito à autorização para o faturamento, a cargo do Gestor do Contrato, e a respectiva ciência do preposto quanto a esta autorização>.

5 – AUTORIZAÇÃO PARA FATURAMENTO
GESTOR DO CONTRATO
Nos termos da alínea "n", inciso I, art. 33, da IN SGD/ME nº 94/2022, AUTORIZA-SE a **CONTRATADA** a <faturar os serviços executados / apresentar as notas fiscais dos bens entregues> relativos à supracitada <OS/OFB>, no valor discriminado no item 4, acima. _____ <Nome do Gestor do Contrato> **Matrícula:** xxxxxxxx <Local>, <dia> de <mês> de <ano>

7 – CIÊNCIA
PREPOSTO
_____ <Nome do Preposto do Contrato> **Matrícula**: xxxxxxx <Local>, <dia> de <mês> de <ano>

Anexo VII - Termo de Recebimento Provisorio.pdf

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Histórico de Revisões

Data	Versão	Descrição	Autor
DD/MM/AAAA	1.0	Primeira versão do documento.	XXXXXXXXXXX

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

<Nas contratações de licenciamento de softwares, é imprescindível verificar se toda a documentação entregue pela contratada está completa e corresponde exatamente ao que foi especificado no TR. É fundamental certificar-se de que todas as licenças, suporte e/ou garantia entregues estejam de acordo com os **part numbers** especificados no TR>.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

TERMO DE RECEBIMENTO PROVISÓRIO – COMPRAS DE TIC

INTRODUÇÃO
O Termo de Recebimento Provisório declarará, de forma sumária, que as compras foram entregues, para verificação posterior da conformidade do material com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato. **Referência: Inciso XXI, art. 2º, e alínea "i", inciso II, art. 33 da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S) E VOLUMES DE EXECUÇÃO			
SOLUÇÃO DE TIC			
<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>			
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**
1	<Descrição igual ao da OFB de abertura>	<Ex.: UNID.>	<n>
...	...	...	...
...	...	...	...
...	...	...	...
TOTAL DE ITENS			

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

3 – RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea "i", da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os <bem(s)/produto(s)> correspondentes à <OFB> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram entregues, estando sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo destes <bem(s)/produto(s)> ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

4 – ASSINATURA

FISCAL TÉCNICO

_____
<Nome do Fiscal Técnico do Contrato>
Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.

PREPOSTO

_____
<Nome do Preposto do Contrato>
Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.