TERMO DE REFERÊNCIA 6/2023

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
6/2023	370003-COORD. GERAL, DE LIC. CONT. E DOC /DGI/SE/CGU	FABRICIO SANTOS DE BRITO	26/12/2023 10:06 (v 0.20)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC	90232/2022	00190.102879/2023-38

1. Termo de Referência

1. DO OBJETO DA CONTRATAÇÃO

1.1. Contratação de serviço de uso de 28 Next Generation Firewall (NGFW) físicos (2 para Sede e 26 para regionais) com funcionalidade de SD-WAN, pelo período de 40 (quarenta) meses, prorrogável por até 120 meses (10 anos), na forma dos artigos 106 e 107 da Lei nº 14.133 de 2021, serviço de implantação e migração da solução atual com repasse de conhecimento, garantia e suporte do fabricante 24/7 com direito de atualização do produto durante a vigência do contrato, 300 horas de serviço de consultoria especializada do fabricante, solução de gerência centralizada e solução de gerenciamento e armazenamento de logs, para a Controladoria-Geral da União – CGU, conforme especificações indicadas nos itens abaixo.

Lote	Item	Descrição	CATSER	Qtde	Unidade
1	1	**NGFW Tipo 1 - Suporte 24/7 por 36 meses - 2 equipamentos de firewall**	**27073**	36	mês
	2	**NGFW Tipo 2 - Suporte 24/7 por 36 meses - 13 equipamentos de firewall**	**27073**	36	mês
	3	**NGFW Tipo 3 - Suporte 24/7 por 36 meses - 13 equipamentos de firewall**	**27073**	36	mês
	4	**Solução de gerência centralizada**	**27073**	36	mês
	5	**Solução de armazenamento e gerência de logs**	**27073**	36	mês
	6	**Implantação da Solução com migração da Atual no ambiente on-premisses**	**13684**	1	unidade
	7	**Repasse de conhecimento - 60 horas**	**16837**	1	unidade
	8	**Serviço técnico especializado do fabricante**	**25631**	300	horas

1.2. O serviço objeto desta contrataçaõ saõ caracterizados como comuns, uma vez que podem ser objetivamente especificados por meio de padroẽs usuais no mercado.

1.3. O prazo de vigeência da contrataçaõ é de 40 (quarenta) meses contados da assinatura do contrato, prorrogável para até 10 anos (120 meses), na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

1.3.1 Apesar do contrato possuir vigência de 40(quarenta) meses, a previsão é que a implantação do serviço ocorra em 4 (quatro meses) e a prestação do serviço contratado ocorra por 36 meses, perfazendo o total da vigência do contrato. Por essa razão, o objeto possui apenas 36 unidades (meses) para os itens de pagamento mensal (itens 1 a 5).

1.3.2. O serviço é enquadrado como continuado tendo em vista que são essenciais para a Controladoria-Geral da União cumprir a sua missão institucional. A utilização de serviços de firewall, para acessar à internet, é essencial para a manutenção das atividades do órgão em todas as suas áreas, pois a sua indisponibilidade impediria o órgão de realizar desde suas atividades mais básicas operacionais até os seus objetivos estratégicos com a segurança de dados necessária. Dessa forma, fica demonstrada a caracterização dos serviços de firewall para acessar à internet como serviço de fornecimento contínuo, conforme a legislação.

1.3.3. Como o serviço de firewall é um serviço de fornecimento contínuo, a interrupção da sua prestação acarretaria enormes prejuízos para a CGU e, por consequência, para o cidadão e para a sociedade. Assim, a finalização da vigência no dia 20 de maio de 2024 do Contrato Administrativo nº 05/2019 obriga a CGU a realizar novo processo de contratação até esta data para evitar qualquer indisponibilidade no serviço de firewall para acesso à internet da CGU.

1.4. Os itens foram agrupados em lote devido a interdependência tecnológica e necessidade de gerência centralizada da solução que se pretende contratar. Dessa forma, justifica-se o agrupamento dos itens pois se trata de uma solução unificada de TIC, cujos itens integrantes são interdependentes. A divisão em lotes acarretaria a não uniformidade da prestação do serviço, dificuldade na gestão dos contratos e fiscalização dos serviços além da perda de economia de escala.

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

1.6. Registramos que devido ao valor estimado e natureza do objeto a ser contratado, serviço de Next Generation Firewall, essa licitação será regida pela INSTRUÇÃO NORMATIVA SGD/ME Nº 94, DE 23 DE DEZEMBRO DE 2022 .

1.7. Ainda, dado que o valor estimado da contratação é inferior a R$ 20(vinte) milhões de reais, não haverá necessidade de submete o processo para aprovação do órgão central do SISP, conforme definido no Art. 2° da INSTRUÇÃO NORMATIVA SGD/MGI No 6, DE 29 DE MARÇO DE 2023.

1.8. Por fim, informo que:

1.8.1. O objeto da contratação em comento não incide nas hipóteses vedadas pelos seus Arts. 3° e 4° INSTRUÇÃO NORMATIVA SGD/MGI N° 6, DE 29 DE MARÇO DE 2023.

1.8.2. A Administração registrou que o objeto da contratação NÃO incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD nº 94/2022.

1.8.3. Na elaboração do edital e de seus anexos foram observadas as vedações do art. 5º da IN SGD nº 94/2022.

1.8.4 Durante a elaboração desse Termo de Referência, foi observado os guias, manuais e modelos publicados pelo Órgão Central do SISP

2. DESCRIÇÃO DA SOLUÇÃO

2.1. A solução de TIC consiste na contratação de serviço para uso de 28 NGFW físicos (2 para Sede com e 26 para regionais) com garantia e suporte do fabricante 24/7 com direito de atualização do produto durante a vigência do contrato, um serviço de implantação e migração da solução atual,

um repasse de conhecimento, uma solução de gerência centralizada e uma solução de gerência e armazenamento de logs, conforme especificações técnicas detalhadas no Anexo I deste Termo de Referência.

3. DA FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A Controladoria-Geral da União (CGU) possui 28 datacenters on-premises, um em cada capital do Brasil, além do seu principal datacenter físico na Sede/DF (Serpro). O contrato CGU n° 05/2019 provê a interconectividade de rede e segurança de perímetro para esta infraestrutura on-premises entre todos estes datacenters. Atualmente este contrato está em seu 3º aditivo, sem possibilidade de nova renovação e a sua vigência final é 20/05/2024.

3.2. Os datacenters da Sede e Regionais estão com o intenso uso de aplicações de vídeo e demais tráfego de sistemas e serviços. Assim, a equipe de redes tem tratado cenários de picos e congestionamento de tráfego nas interfaces dos equipamentos de rede. Por isso, estão em fase final novos projetos de expansão da capacidade de tráfego de conectividade através do mudanças nas arquiteturas de rede, incremento de links e interfaces de todos os equipamentos redes destes ambientes.

3.3. Adicionalmente a infraestrutura e interconexões tradicionais entre datacenters físicos on-premises, a CGU iniciou a sua jornada para nuvem, por meio do contrato CGU nº 21/2019 com a empresa Claro. Esse contrato fornece os serviços de nuvem da Amazon Web Services (AWS) que já abriga os principais sistemas externos críticos da Organização, como FalaBr, Portal da Transparência, SISCOR, e-PAD, SeCI etc. Além desses serviços de nuvem da AWS, a CGU também utiliza os serviços de nuvem da Microsoft do Office 365, por meio do contrato nº 16/2020, para soluções escritório digital, como correio eletrônico (outlook), armazenamento de arquivos (sharepoint), comunicações (Teams) etc. Formou-se então um cenário híbrido on-premises e multicloud (AWS e Azure) de múltiplas contas, onde emerge como um novo desafio para segurança de perímetro e gerenciamento de vulnerabilidades, com a utilização de tecnologias diversas, providas por fabricantes distintos, com níveis de proteções diferentes, a depender das limitações das soluções de segurança disponíveis em cada ambiente, e a garantia de compliance nas múltiplas contas de nuvem nos seus ambientes de nuvens distintos. Por fim, neste tipo de ambiente, as arquiteturas têm se tornado cada vez mais complexas e mão de obra altamente especializada se faz cada vez mais necessária.

3.4. Para a preservação da continuidade do serviço essencial de segurança de perímetro on-premises atual, busca-se a contratação de:

3.4.1. 28 Next Generation Firewall (NGFW) físicos (2 para Sede e 26 para regionais), com solução de VPN moderna com autenticação com 2FA para acessos administrativos;

3.4.2. serviço de implantação com a migração da solução on-premises atual;

3.4.3. repasse de conhecimento para a equipe técnica da CGU;

3.4.4. serviço de gerenciamento centralizado;

3.4.5. serviço de armazenamento e gerenciamento de logs;

3.4.6. Solução com suporte técnico 24x7 com garantia e direito de atualização do produto pelo fabricante durante a vigência do contrato;

3.5. Para garantir a modernização da infraestrutura tecnológica de ambiente do ambiente híbrido da CGU, os seguintes requisitos de negócio abaixo devem ser alcançados:

3.5.1. solução unificada que promova garantia do mesmo nível de compliance de segurança em toda a infraestrutura híbrida (on-premises e nuvem), fornecendo os mesmos mecanismos de detecção e prevenção de ameaça;

3.5.2. horas de consultoria com engenheiro especializado do fabricante, no intuito de sempre ter um apoio especializado que possa orientar, planejar e implantar as melhores recomendações em segurança no desenvolvimento de novas arquiteturas com a solução on-premises ou em nuvem;

3.6. Para atender novos projetos de conectividades de rede da Organização, apresentados no Estudo Técnico Preliminar, também são requisitos da contratação:

3.6.1. segurança de perímetro para todos os datacenters “on-premises” (regionais e sede) compatível com solução de interconectividade para garantir a alta disponibilidade dos links de Internet (Firewall + SD Wan);

3.6.2. NGFW tenham interfaces de rede de 25Gbase-sr para Sede e interfaces de 10GBase-sr para as Regionais.

3.6.3. independência do componente de virtualização das regionais;

3.7. Ademais, entende-se como presentes na solução de NGFW todas as características de segurança abaixo:

3.7.1. possuir as seguintes características de controle e fluxo de dados: mecanismos de Quality of Service (QoS), como deduplicação, compressão, cache, marcação de pacotes e “traffic shaping” para classificação, segmentação, otimização, aceleração, priorização do tráfego de rede e possibilitar a criação túneis criptografados via IPSec entre sites;

3.7.2. possuir as seguintes características de segurança: inspeção de tráfego em camada nível 7; Intrusion Detection System (IDS); Intrusion Prevention System (IPS); deteção antimalware avançada (sandbox), Web Filterning;

3.7.3. possuir política de roteamento com protocolo Border Gateway Protocol (BGP);

3.8. Desta forma, a solução a ser contratada é o serviço para uso de 28 NGFW físicos (2 para Sede e 26 para as regionais) com funcionalidade de SD-WAN, um serviço de implantação e migração da solução atual, repasse de conhecimento, e garantia e suporte do fabricante 24/7 com direito de atualização do produto durante a vigência do contrato, 300 horas de serviço de consultoria especializada do fabricante, solução de gerência centralizada e solução de gerenciamento e armazenamento de logs.

3.9. Conforme Informações detalhadas no Estudo Técnico Preliminar desta contratação, os quadros finais com a volumetria desta contratação são apresentados abaixo.

3.9.1. Para os Itens 1,2 e 3, a tabela abaixo apresenta as capacidades mínimas de Throughput com Threat Prevention estimadas para cada ambiente de NGFW físicos on-premises e é apresentado o cálculo do número estimado de usuários que irão utilizar a solução de VPN com 2FA.

Categoria	Ambiente	Localidade	Forma	Quantidade	Capacidade Mínima / Throughput Threat Prevention (Gbps)	Capacidade Mínima / Throughput NGFW (Gbps)	Requisitos mínimos para interfaces
Tipo 1	On-premises	Sede/DF	Físico	2	12.5	22	2x25Gbps

Tipo 2	On-premises	Regionais	Físico	13	2.2	3.9	4x10Gbps
Tipo 3	On-premises	Regionais	Físico	13	1.8[TGP1]	3.2	4x10Gbps

Tabela de Quantitativos e Capacidades dos Equipamentos de Firewalls do ambiente on-premises (Sede e Regionais)

3.9.2. Para o Item 1, a quantidade de usuários simultâneos com acesso à VPN com 2FA é de 92.

3.9.3. Para o Item 4, solução de gerenciamento centralizado, a quantidade estimada de dispositivos a serem gerenciados são de 37.

3.9.4. Para o item 5, solução de gerência e armazenamento de logs, a quantidade estimada de 45 GB/dia.

3.9.5. Para o Item 8, horas para consultoria especializada do fabricante, foram estimadas 300 horas para planejamento ou implantação de futuros projetos de soluções (on-premises ou em nuvem, Azure e AWS) de novas arquiteturas, funcionalidades no ambiente da CGU.

3.10. As justificativas para os quantitativos supracitados estão no Estudo Técnico Preliminar desta contratação.

3.11. A presente contratação visa a alcançar os principais resultados e benefícios:

3.11.1. continuidade do serviço essencial de proteção de perímetro a toda infraestrutura de TI, Firewall e SD-WAN, que sustenta todos os sistemas e dados on-premises desta Organização, como os sistemas críticos Super, E-aud etc.;

3.11.2. adquirir solução on-premises que seja compatível com tecnologias de nuvem AWS e Microsoft Azure, de forma a nivelar e centralizar os mecanismos de detecção e prevenção de ameaças de segurança cibernética em toda a nova infraestrutura híbrida, “on-premises” e “multicloud”;

3.11.3. garantir a modernização da infraestrutura tecnológica da CGU e adequação às constantes evoluções na área de tecnologia da informação;

3.11.4. Ampliação da segurança dos dados institucionais.

3.12. O objeto da contrataçaõ está previsto no Plano de Contrataçoẽs Anual 2023, conforme detalhamento a seguir:

1. DFD 345/2022.
2. ID PCA no PNCP: 26664015000148-0-000001/2023;
3. Data de publicaçaõ no PNCP: 20/05/2023;
4. Id dos itens no PCA: 37 (trinta e sete)
5. Classe/Grupo: 163 - SERVIÇOS DE HOSPEDAGEM EM TECNOLOGIA DA INFORMAÇÃO E COMUNICACÃO (TIC);
6. Identificador da Futura Contrataçaõ: 370003-232/2022;

3.13. O objeto da contrataçaõ também está alinhado com a Estratégia de Governo Digital 2020-2023 e em consonância com o Plano Diretor de Tecnologia da Informaçaõ e Comunicaçaõ (PDTIC) 2023-2024 da CGU, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS

ID	Objetivos Estratégicos
13	**Objetivo 13:** Racionalizar os recursos logísticos, financeiros e de TIC, com foco na sustentabilidade, segurança e efetividade.

ALINHAMENTO AO PDTIC 2023 - 2024			
ID	Ação do PDTIC	**ID**	Meta do PDTIC associada
13.3	Estabelecer e aprimorar o gerenciamento dos níveis de serviço de TIC.	**5.1**	Planejar a gestão de tecnologia da Informação

4. REQUISITOS DA CONTRATAÇÃO

4.1.Requisitos do Negócio

4.1.1. São requisitos de negócio desta contratação:

4.1.1.1. solução unificada que promova garantia do mesmo nível de compliance de segurança em toda a infraestrutura híbrida (on-premises e nuvem), fornecendo os mesmos mecanismos de detecção e prevenção de ameaça, com solução de VPN moderna com autenticação com 2FA para acessos administrativos;

4.1.1.2. serviço de implantação com a migração da solução on-premises atual;

4.1.1.3. repasse de conhecimento para a equipe técnica da CGU;

4.1.1.4. serviço de gerenciamento centralizado;

4.1.1.5. serviço de armazenamento e gerenciamento de logs;

4.1.1.6. horas de consultoria com engenheiro especializado do fabricante, no intuito de sempre ter um apoio especializado que possa orientar, planejar e implantar as melhores recomendações em segurança no desenvolvimento de novas arquiteturas com a solução on-premises ou em nuvem;

4.1.1.7. solução com suporte técnico 24x7 com garantia e direito de atualização do produto pelo fabricante durante a vigência do contrato;

4.1.1.8. segurança de perímetro para todos os datacenters “on-premises” (regionais e sede) compatível com solução de interconectividade para garantir a alta disponibilidade dos links de Internet (Firewall + SD Wan);

4.1.1.9. independência do componente de virtualização das regionais;

4.2. Requisitos Legais

4.2.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Lei n° 10.520, de 17 de julho de 2001, Decreto 10.024, de 20 de setembro de 2019, e a outras legislações aplicáveis;

4.2.2. Diretrizes para a Contratação de Serviços em Nuvem, publicado em 13/05/16, disponível em https://www.gov.br/governodigital/pt-br/contratacoes/Orientacaoservicosemnuvem.pdf;

4.3. Requisitos de Manutenção

4.4.1. A Solução de Tecnologia da Informação deverá prover serviços de manutenção preventiva, corretiva, evolutiva e adaptativa, pois será necessário que a contratada responda por todos os vícios e defeitos dos serviços durante o período de vigência do contrato.

4.4.1.1. A correção de erros dos softwares deve ser realizada sem ônus à contratante, durante o prazo de validade técnica dos softwares, nos termos do Capítulo III da Lei nº 9.609/1998. Caso os erros venham a ser corrigidos em versão posterior do software, essa versão deverá ser fornecida sem ônus para a contratante.

4.4.2. O Suporte de todos os equipamentos de hardware e soluções de software deverão estar vigentes no fabricante e estar disponíveis em regime 24 x 7 (vinte e quatro horas por dia e sete dias por semana) durante toda a vigência do contrato.

4.4.3. Todos os equipamentos de hardware e os licenciamentos de software deverão estar com as garantias ativas no fabricante da solução durante toda a vigência do contrato.

4.4.4. Demais requisitos de manutenção (garantia e suporte técnico) estão definidos nos ANEXOS I e II.

4.4. Requisitos Temporais

4.4.1. A entrega dos equipamentos deverá ser efetivada no prazo máximo de 60 (sessenta) dias corridos, a contar da emissão da ordem de serviço.

4.4.2. Toda a solução contratada deverá estar implantada e migrada no prazo máximo de 120 (cento e vinte) dias corridos, contados a partir da emissão da ordem de serviço.

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

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

4.4.5. Os demais prazos, tanto para a entrega dos equipamentos quanto para a prestação dos serviços, encontram-se descritos no item 8 "Modelo de Execução do Contrato" deste termo de referência e no ANEXO I.

4.5. Requisitos de Segurança e Privacidade

4.5.1. A CONTRATADA deverá respeitar a classificação das informações produzidas ou custodiadas pela CGU que vier a ter acesso por necessidade do serviço.

4.5.2. Boas práticas relativas à segurança da informação durante a implantação da solução contratada.

4.5.3. A CONTRATADA deve providenciar cópia para todos os profissionais alocados na execução dos serviços da Política Corporativa de Segurança da Informação da CGU e das demais normas disponibilizadas pela CGU, bem como zelar pela observância dessas normas.

4.6. Requisitos de Sociais, Ambientais e Culturais

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

4.6.1.1. Os relatórios deverão ser elaborados de forma eletrônica, evitando a confecção e transporte de mídias.

4.6.1.2. Os softwares desenvolvidos deverão ser fornecidos com interfaces em língua portuguesa brasileira ou com possibilidade de configuração para o português do Brasil.

4.6.2. Além dos critérios de sustentabilidade eventualmente inseridos no item acima, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis, elaborado pela Câmara Nacional de Sustentabilidade da Consultoria Geral da União/Advocacia Geral da União :

4.6.2.1. Somente poderão ser utilizados na execução dos serviços bens de informática e/ou automação 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.

4.6.2.2. Somente poderão ser utilizados na execução dos serviços bens de informática e/ou automação que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs).

4.6.3. Os equipamentos devem estar aderentes à Lei nº 12.305, de 2 de agosto de 2010, que Institui a Política Nacional de Resíduos Sólidos.

4.6.4. No que couber, visando a atender ao disposto na legislação aplicável – em destaque às Instruções Normativas nº 05/2017/SEGES e nº 01/2019/SGD – a CONTRATADA deverá priorizar, para o fornecimento do objeto, a utilização de bens que sejam no todo ou em parte compostos por materiais recicláveis, atóxicos e biodegradáveis.

4.7. Requisitos de Arquitetura Tecnológica

4.7.1. Os equipamentos fornecidos deverão ser novos, originais de fábrica (não podem ter sido recondicionados), de primeiro uso, da geração na respectiva linha de produtos do fabricante.

4.7.2. Os equipamentos deverão ser idênticos aos da proposta comercial da licitação. Qualquer alteração deverá ser expressamente autorizada pela CONTRATANTE.

4.7.3. As soluções de gerenciamento centralizado e a solução de gerência e armazenamento de logs deverão ser do mesmo fabricante dos equipamentos de NGFW ofertados;

4.7.4. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas nas Especificações Técnicas do ANEXO I.

4.8. Requisitos de Implantação e Migração

4.8.1. Para a execução do item de Implantação e Migração da Solução atual, a contratada deverá apresentar um gerente de projetos e um responsável técnico com, no mínimo, a experiência profissional, formação acadêmica e certificação descritas para cada perfil abaixo.

4.8.1.1. A CONTRATADA deverá indicar um gerente de projetos, com no mínimo, o perfil abaixo.

PERFIL 01 – Gerente de Projeto da Implantação e Migração	
Responsável pelo planejamento e acompanhamento de todas as atividades, controle de prazos, esforço, elaboração de relatórios de posicionamento executivo, indicadores do projeto.	
Experiência Profissional	**Modo de Comprovação**
Experiência mínima de 02 (dois) anos em gerenciamento de projetos.	Declaração emitida e assinada por Pessoa Jurídica de direito público ou privado que comprove a participação do funcionário na execução das atividades correlatas.
Qualificação Técnica	**Modo de Comprovação**
Certificação Project Management Professional (PMP) ou similares.	Cópia da Certificação, com código e o link para validação no sítio da instituição certificadora.
Formação Escolar/Acadêmica	**Modo de Comprovação**
Curso superior completo, em qualquer área.	Cópia do Diploma, devidamente registrado, de conclusão de curso de graduação em nível superior em qualquer área fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.

4.8.1.2. A CONTRATADA deverá indicar um responsável técnico, com no mínimo, o perfil abaixo:

PERFIL 02 – Responsável Técnico pela Implantação e Migração da Solução Atual	
Responsável por conduzir e acompanhar todas as atividades técnicas e operacionais durante as atividades de implantação e migração da solução atual.	
Experiência Profissional	**Modo de Comprovação**
Experiência mínima de 03 (três) [MD1] [TGP2] anos em soluções de firewall.	**Declaração emitida e assinada por Pessoa Jurídica** de direito público ou privado que comprove a participação do funcionário na execução das atividades correlatas.
Qualificação Técnica	
Certificação avançada ou profissional ou de administrador oficial do fabricante na solução de firewall ofertada.	Cópia da Certificação, com código e o link para validação no sítio da instituição certificadora.

Formação Escolar /Acadêmica	Modo de Comprovação
Curso superior completo na área de Tecnologia da Informação.	Cópia do Diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou mestrado ou doutorado, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.

4.8.1.3. A CONTRATADA deverá indicar o instrutor do repasse de conhecimento, com no mínimo, o perfil abaixo:

PERFIL 03 – Instrutor do Repasse de Conhecimento	
Responsável por conduzir o repasse de conhecimento à CONTRATANTE, conforme definições das Especificações Técnicas do ANEXO I.	
Qualificação Técnica	**Modo de Comprovação**
Certificação avançada ou profissional ou de administrador oficial do fabricante na solução de firewall ofertada.	Cópia da Certificação, com código e o link para validação no sítio da instituição certificadora.
Formação Escolar /Acadêmica	**Modo de Comprovação**
Curso superior completo na área de Tecnologia da Informação.	Cópia do Diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou mestrado ou doutorado, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.

4.8.2. Ainda, maiores detalhes sobre a Implantação e Migração da Solução atual estão descritos nas Especificações Técnicas do ANEXO I e no item 8 - Modelo da Execução do Contrato, deste Termo de Referência.

4.9. Requisitos de Garantia Contratual

4.9.1. Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021, uma vez que não haverá pagamento adiantado pelo serviço a ser prestado.

4.10. Demais Requisitos

4.10.1. Comprovação da origem dos bens importados, caso ocorra, oferecidos e da quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto, sob pena de rescisão contratual e multa, em atendimento ao inciso III do art. 3º do Decreto 7.174/2010;

5. DA VISTORIA PARA LICITAÇÃO

5.1. Para o correto dimensionamento e elaboração de sua proposta, o LICITANTE poderá, a seu critério, realizar vistoria, acompanhado por servidor designado para esse fim;

5.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até dois dias úteis anterior à data prevista para a abertura da sessão pública;

5.3. Nesta oportunidade, serão respondidas dúvidas sobre o ambiente de firewall da CGU.

5.4. A vistoria poderá ser realizada em dias úteis, das 9h às 11h e das 14h às 17h, devendo o agendamento prévio ser realizado pelo e-mail cgetc@cgu.gov.br ou pelo telefone (61) 2020-7053, com antecedência mínima de 24 (vinte e quatro) horas;

5.5. A vistoria poderá ser realizada de forma remota, utilizando tecnologia de videoconferência, compartilhamento de desktop ou outra forma a combinar;

5.6. Em nenhuma hipótese a LICITANTE poderá alegar desconhecimento, incompreensão, dúvidas ou esquecimento de qualquer detalhe relativo ao objeto, responsabilizando-se por quaisquer ônus decorrentes desses fatos.

6. DA SUBCONTRATAÇÃO E DO CONSÓRCIO

6.1. Será permitida a subcontratação do item de repasse de conhecimento, uma vez que o mercado apresenta empresas especializadas no assunto. O item de repasse de conhecimento está agrupado com os demais itens pois é necessária a definição da solução ofertada para promover a capacitação adequada;

6.2. No caso de subcontratação a licitante continuará como responsável pelos serviços prestados, não podendo imputar a terceiros a culpa por qualquer descumprimento contratual.

6.3. A contratação do item 8, Serviço Técnico Especializado do Fabricante, não é considerada subcontratação uma vez que este tipo de serviço apenas é comercializado através de empresas parceiras.

6.4. É vedada a participaçaõ de pessoas jurídicas reunidas em consórcio ou cooperativas para participaçaõ do certame da presente contrataçaõ.

> 6.4.1 Isso se justifica pois a Equipe de Planejamento da Contrataçaõ (EPC) identificou em Estudos Técnicos Preliminares (ETP) que há no mercado múltiplos fornecedores capazes de atender a integralidade do objeto da contrataçaõ, desse modo, resta claro que a vedaçaõ da participaçaõ de consórcios e cooperativas naõ comprometera a competitividade da licitaçaõ.

7. DAS RESPONSABILIDADES

7.1. DAS OBRIGAÇÕES DA CONTRATANTE

7.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

7.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço, de acordo com os critérios estabelecidos no Termo de Referência;

7.1.3. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

7.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

7.1.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

7.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

7.1.7. Permitir o acesso dos empregados da CONTRATADA às dependências da CONTRATANTE, mediante identificação, para prestação de serviço.

7.1.8. Prestar as informações e esclarecimentos relativos ao objeto desta contratação que venham a ser solicitados pelo preposto da CONTRATADA.

7.2. DAS OBRIGAÇÕES DA CONTRATADA

7.2.1. Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato;

7.2.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

7.2.3. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

7.2.4. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

7.2.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

7.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

7.2.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e

7.2.8. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

7.2.9. Fazer a transição contratual, quando for o caso, observado o disposto no art. 35 da IN SGD nº 94, de 23 de dezembro de 2022;

7.2.10. Apresentar os empregados devidamente identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso.

7.2.11. Apresentar à CONTRATANTE, quando for o caso, a relação nominal dos empregados que adentrarão nas dependências do órgão e unidades vinculadas para a execução do serviço.

7.2.12. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.

7.2.13. Refazer os serviços que forem considerados insatisfatórios em relação aos parâmetros contratuais estabelecidos, sem qualquer custo adicional para a CONTRATANTE.

8. DO MODELO DE EXECUÇÃO DO CONTRATO

8.1 A execução do objeto seguirá a seguinte dinâmica:

Prazo para início da prestação dos serviços

8.1.1. Para os itens de 1 a 6 contratados, a CONTRATADA deverá entregar estes serviços implantados e totalmente operacionais, em até 120 (cento e vinte) dias corridos após a emissão da Ordem de Serviço.

8.1.1.1. Para o item 7 a CONTRATADA deverá entregar este serviço, em até 35(trinta e cinco) dias corridos após a emissão da Ordem de Serviço, conforme cronograma da tabela do item 9.29 deste Termo de Referência.

8.1.1.2. Para o item 8 a CONTRATADA deverá entregar este serviço, em até 10(dez) dias corridos após a emissão da Ordem de Serviço.

Local da prestação dos serviços

8.1.2. Sede - Brasília/DF, os equipamentos deverão ser entregues e o serviço deverá ser prestado nos seguintes endereços: Datacenter do SERPRO REGIONAL BRASÍLIA - SGAN L2 Norte Quadra 601 Módulo G - CEP: 70836-900.

8.1.2.1. Para acesso físico aos Datacenters da Sede (Brasília/DF) e das Regionais para a entrega, instalação e configuração dos equipamentos é necessário disponibilizar as informações de nome e documento de identificação de todas as pessoas que irão executar o serviço de implantação.

8.1.2.2. Acesso aos Datacenters deverão ser agendados com a equipe técnica da CGU com pelos menos 48 (quarenta e oito) horas de antecedência.

8.1.2.3. Caso os profissionais necessitem de entrar no ambiente de datacenter com equipamentos de informática (notebook, entre outros), para apoiar na instalação dos equipamentos, as informações dos equipamentos deverão ser repassadas juntamente com as informações do item anterior, para agilizar a liberação da entrada no datacenter.

8.1.3. Nas regionais da CGU, os equipamentos deverão ser entregues e o serviço deverá ser prestado nos seguintes endereços: https://www.gov.br/cgu/pt-br/acesso-a-informacao/institucional/quem-e-quem/unidades-regionais-da-controladoria-geral-da-uniao

8.1.3.1 Em caso de mudança de endereço de entrega, o novo endereço será repassado para a CONTRATADA;

8.1.4. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 25 (vinte e cindo) dias úteis, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

Disponibilização de infraestrutura para a contratada

8.1.5. A CONTRATANTE disponibilizará espaço em rack para os equipamentos e alimentação de energia. E disponibilizará também a infraestrutura de TI de máquinas virtuais, conforme requisitos definidos pela CONTRATADA, para implantação dos serviços de gerenciamento centralizado e gerência e armazenamento de logs;

8.1.6. Na Sede/DF, a CONTRATANTE disponibilizará colaboradores da operação terceirizada indicados para acompanhar a implantação e as atividades de migração com disponibilidade:

8.1.6.1. Presencial: com disponibilidade em dias úteis em horário comercial (8 – 17h);

8.1.6.2. Remota: 24x7;

8.1.7. Nas Regionais, a CONTRATANTE disponibilizará capacidade operacional de apoio técnico local que poderão receber as devidas orientações técnicas da CONTRATADA para auxiliar o apoio físico na regional, com disponibilidade em dias úteis em horário comercial (8 – 17h);

Procedimento de transição e finalização de contrato

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

Mecanismos Formais de Comunicação

8.1.9. São definidos como mecanismos formais de comunicação, entre a CONTRATANTE e a CONTRATADA, os seguintes:

8.1.9.1. Ordem de Serviço (OS);

8.1.9.2. Ata de Reunião;

8.1.9.3. Ofício;

8.1.9.4. E-mail.

Quantidade de serviços

8.1.10 Cada OS conterá o volume de serviços demandados, incluindo a sua localização e o prazo, conforme modelo descrito no ANEXO V - MODELO DE ORDEM DE SERVIÇO desse Termo de Referência.

Manutenção de Sigilo e Normas de Segurança

8.1.11. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução 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.

9. DO MODELO DE GESTÃO DO CONTRATO

9.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei n° 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

9.2. 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.

9.3. 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.

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

Reunião inicial

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

9.6. A reuniaõ seraá realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME no 94, de 2022, e ocorreraá em ateé 10 (dez) dias uteis da assinatura do Contrato, podendo ser prorrogada a criteério da Contratante.

9.6.1. A pauta desta reuniaõ observaraá, pelo menos:

9.6.1.1. Presença do representante legal da contratada, que apresentaraá o seu preposto;

9.6.1.2. Entrega, por parte da CONTRATADA, do Termo de Compromisso de Confidencialidade e dos Termos de Cieência;

9.6.1.3. esclarecimentos relativos a questoẽs operacionais, administrativas e de gestaõ do contrato;

9.7. A reunião poderá ser on-line ou presencial, a critério das partes.

Fiscalização

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

Fiscalização Técnica

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

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

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

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

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

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

Fiscalização Administrativa

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

9.10.1. Caso ocorra 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).

Gestor do Contrato

9.11. 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).

9.12. 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).

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

9.14. 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).

9.15. 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).

9.16. 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).

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

Do recebimento e aceitação do objeto

9.18. O recebimento provisório se dará mediante confecção e assinatura do Termo de Recebimento Provisório, a cargo do Fiscal Técnico do Contrato, quando da entrega do objeto constante na Ordem de Serviço (OS), que ocorrerá em até 15(quinze) dias úteis para os itens 1 a 6 e de 05 (cinco) dias úteis para o item 7 e 8;

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

9.20. Em caso de verificação de desconformidade será dado encaminhamento das demandas de correção à contratada, a cargo do Gestor do Contrato ou, por delegação de competência, de membro da Equipe de Fiscalização do Contrato;

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

9.22. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14.133, de 2021).

9.23. Os serviços serão recebidos definitivamente nos prazos de 15 (quinze) dias úteis para os itens 1 a 6 e de 05 (cinco) dias úteis para o item 7, 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:

9.23.1. Avaliação da qualidade dos serviços realizados e justificativas, a partir da aplicação dos procedimentos de teste e inspeção, de acordo com os critérios de aceitação e dos níveis mínimos de serviço exigidos, a cargo dos Fiscais Técnico e Requisitante do Contrato;

9.23.2. 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;

9.23.3. Confecção e assinatura do Termo de Recebimento Definitivo, a cargo do Fiscal Requisitante, Fiscal Técnico do Contrato e Gestor do Contrato;

9.23.4. Autorização para o faturamento e emissão de nota fiscal com valor dimensionado pela fiscalização, a cargo do Gestor do Contrato com base no Termo de Recebimento Definitivo, a ser encaminhada ao preposto da contratada;

9.24. 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.

9.25. 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 se refere à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

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

9.27. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço, a responsabilidade ético-profissional pela perfeita execução do contrato nem pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor (Lei n° 10.406, de 2002).

Do quadro resumo dos eventos de entrega dos itens.

9.28. A tabela de abaixo apresenta o cronograma de eventos resumidos para os itens de 1, 2, 3, 4, 5 e 6:

Evento	Descrição do evento	Prazo Máximo	Responsável
1	Abertura de Ordem de Serviço (OS)	-	CONTRATANTE
2	Entrega dos equipamentos físicos na Sede/DF e nas Regionais	Evento 1 + 60 dias corridos	CONTRATADA

3	Entrega das comprovações de experiência, certificações e grau de escolaridade dos Gerente de Projetos e Responsável Técnico pela Implantação e Migração	1 dia útil antes do início do evento 4	CONTRATADA
4	Reunião inicial	Evento 1 + 5 dias úteis	CONTRATADA E CONTRATANTE
5	Entrega do Plano de Implantação e Migração	Evento 4 + 20 dias úteis	CONTRATADA
6	Instalação e Configuração para gerenciamento remoto de todos os Equipamentos da Sede/DF e Regionais	Evento 2 + 20 dias úteis	CONTRATADA E CONTRATANTE
7	Recebimento Provisório dos Bens	Evento 6 + 15 dias úteis	CONTRATANTE
8	Fim da Implantação e Migração da Solução Atual, com a entrega da Documentação da Implantação e Migração (as-built)	Evento 1 + 120 dias corridos.	CONTRATADA E CONTRATANTE
9	Emissão de Termo de Recebimento Definitivo	Evento 8 + 15 dias úteis	CONTRATANTE

8.29. A tabela de eventos 2 apresenta o cronograma de eventos resumidos para o item 7 (Repasse de Conhecimento):

Evento	Descrição do evento	Prazo Máximo	Responsável
1	Abertura de Ordem do Serviço (OS)	-	CONTRATANTE
2	Entrega da comprovação de experiência e capacitação do Instrutor do Repasse de Conhecimento	10 dias úteis antes do início do evento 3	CONTRATADA
3	Início do Repasse de Conhecimento	Evento 1 + 35 dias corridos	CONTRATADA E CONTRATANTE
4	Fim Repasse de Conhecimento	-	CONTRATADA E CONTRATANTE
5	Entrega dos certificados de conclusão	Evento 4 + 15 dias corridos	CONTRATADA

6	Avaliação do Repasse de Conhecimento	Evento 4 + 10 dias úteis	CONTRATANTE
7	Termo de Recebimento Provisório do Repasse de Conhecimento	Evento 6 + 5 dias úteis	CONTRATANTE
8	Emissão de Termo de Recebimento Definitivo	Evento 7 + 5 dias úteis	CONTRATANTE

8.30. Os prazos acima poderão ser antecipados a critério do responsável.

8.31. O recebimento do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

8.32. Conteúdo mínimo exigido para a entrega do Plano de Implantação e Migração da Solução atual foi definido nas Especificações Técnicas no ANEXO I.

8.33. Conteúdo mínimo exigido para a entrega da Documentação da Implantação e Migração da Solução atual (as-built) foi definido nas Especificações Técnicas no ANEXO I.

Dos Critérios de medição

9.34. A avaliação da execução do objeto utilizará a apuração dos níveis de serviço realizada após a finalização de cada mês de prestação do serviço (itens 1 a 5), abrangendo a apuração dos indicadores de desempenho da Contratada durante todo o período daquele mês;

9.35. Os níveis mínimos exigidos para essa contratação, bem como o cálculo do desconto a ser aplicado na fatura no caso de não cumprimento dos níveis de serviço exigidos, estão detalhados no ANEXO II - NÍVEIS MÍNIMOS DE SERVIÇO E CÁLCULO DE PAGAMENTO.

9.36. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade identificada, sem prejuízo das sanções cabíveis, caso se constate que a contratada:

9.36.1. não produzir os resultados acordados,

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

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

Da Liquidação

9.37. Os pagamentos referente aos itens 1 a 5 deste Termo de Referência serão feitos em parcela mensal após a emissão dos respectivos Termos de Recebimentos Definitivos.

9.38. Os pagamentos referente aos itens 6 e 7 deste Termo de Referência serão feitos em parcela única após a emissão dos respectivos Termos de Recebimentos Definitivos

9.38.1 Os pagamentos referentes ao item 8 deste Termo de Referência serão feitos em parcelas de acordo com o consumo do item durante a vigência do contrato e após a emissão dos respectivos Termos de Recebimentos Definitivos

9.39. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

9.40. 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:

9.40.1. o prazo de validade;

9.40.2. a data da emissão;

9.40.3. os dados do contrato e do órgão contratante;

9.40.4. o período respectivo de execução do contrato;

9.40.5. o valor a pagar; e

8.40.6. eventual destaque do valor de retenções tributárias cabíveis.

9.41. 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;

9.42. 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.

9.43. 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. (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018)

9.44. 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.

9.45. 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.

9.46. 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.

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

Prazo de pagamento

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

9.49. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação 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, assim apurado:

TX = 6% ao ano

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

Forma de pagamento

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

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

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

9.53. 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.

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

Cessão de crédito

9.55. 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.

9.55.1. As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.

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

9.57. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

9.58. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020).

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

SANÇÕES ADMINISTRATIVAS

9.60. Comete infração administrativa nos termos da Lei n° 14.133, de 2021 a CONTRATADA que:

9.60.1. dar causa à inexecução parcial do contrato;

9.60.2. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

9.60.3. dar causa à inexecução total do contrato;
9.60.4. deixar de entregar a documentação exigida para o certame;

9.60.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

9.60.6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.60.7. ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

9.60.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

9.60.9. fraudar a licitação ou praticar ato fraudulento na execução do contrato;

9.60.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

9.60.11. praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

9.60.12. praticar ato lesivo previsto no art. 5° da Lei n° 12.846, de 1° de agosto de 2013.

9.61. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

9.61.1. Será penalizado com advertência quando der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave.

9.61.2. Multa de:

9.61.2.1. moratória de 1,0% (um por cento) sobre o valor da Nota Fiscal, por dia de atraso, observado o máximo de 10% (dez por cento), no caso de descumprimento dos prazos estabelecidos no Termo de Referência, para os quais não haja previsão de penalidade específica;

9.61.2.2. Em caso de reincidência, multa compensatória de 5% (cinco por cento), aplicada cumulativamente, sobre o valor da Nota Fiscal, referente ao mês em que for constatado o novo descumprimento contratual;

9.61.2.3. compensatória de 2,5% (dois e meio por cento) sobre o valor da Nota Fiscal, referente ao mês em que for constatado o descumprimento de qualquer obrigação prevista no Termo de Referência para as quais não tenha sido definida sanção específica;

9.61.2.4. compensatória de 5% (cinco por cento) sobre o valor total da contratação, nos casos de rescisão contratual por culpa da Contratada;

9.61.2.5. Compensatória 25% (vinte e cinco por cento) do valor mensal previsto para o item do objeto, por inexecução parcial do objeto do contrato.

9.61.2.6. Compensatória 2% (dois por cento) do valor anual total do contrato, por inexecução total do objeto do contrato.

9.61.2.7. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

9.61.3. Impedimento de licitar e contratar, quando praticadas as condutas descritas nos subitens 9.60.2 a 9.60.7, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4°, da Lei no 14.133, de 2021);

9.61.4. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nos subitens 9.60.8 a 9.60.12, bem como nos subitens 9.60.2 a 9.60.7, que justifiquem a imposição de penalidade mais grave (art. 156, § 5°, da Lei no 14.133, de 2021);

9.62. As sanções previstas nos itens 9.61.3 e 9.61.4 poderão ser aplicadas à CONTRATADA juntamente com as de multa.

9.63. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei n° 14.133, de 2021, e subsidiariamente a Lei no 9.784, de 1999;

9.64. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

9.65. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

9.65.1. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

9.66. Poderá caracterizar inexecução parcial do contrato:

9.66.1. Descumprimentos de níveis mínimos de serviço no âmbito da mesma Ordem de Serviço que tenham ensejado desconto total igual ou superior a 20% (vinte por cento) do valor de faturamento da OS em dois faturamentos consecutivos ou por três faturamentos alternados em seis períodos de apuração consecutivos da OS.

9.66.2. Não alcance de meta do mesmo indicador de qualidade no âmbito da mesma Ordem de Serviço, em três faturamentos consecutivos ou por quatro faturamentos alternados em seis períodos de apuração consecutivos dessa OS.

9.66.3. Tentativa de burla de mecanismos de aferição dos níveis de serviço previstos neste Termo de Referência.

9.67. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade;

9.68. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei no 12.846, de 1o de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da

responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

9.69. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei no 12.846, de 1o de agosto de 2013, seguirão seu rito normal na unidade administrativa.

9.70. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

10. FORMA E CRITÉRIO DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

10.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço, uma vez que os serviços previstos neste Termo de Referência enquadram-se na definição de bens e serviços comuns do inciso XIII do art. 6o da Lei 14.133/2021.

10.2. O regime de execução do contrato será por preço unitário.

10.3. O critério de julgamento é o menor preço.

10.4. Por se tratar de contratação de serviços continuados e de modo evitar, assim, propostas inexequíveis ou que possam impactar a futura gestão contratual, sugere-se o modo de disputa ABERTO E FECHADO.

Da Aplicação da Margem de Preferência

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

> 10.5.1. Em conformidade com o disposto no art. 4°, §1°, inciso I, da Lei 14.133 /2021, não será aplicado o direito de preferência de que trata os Arts. 42 a 49 da Lei Complementar n° 123/06, tendo em vista que o valor anual estimado da contratação, e superior ao faturamento bruto anual estabelecido para as Empresas de Pequeno Porte (EPP), cujo teto máximo de enquadramento legal corresponde ao montante de R$4.800.000,00 (Quatro milhões, oitocentos mil reais), e, por consequência, ao faturamento das Microempresas (ME), que têm como teto máximo para enquadramento legal o valor de R$360.000,00 (Trezentos e sessenta mil reais).

10.6. Não será aplicada a margem de preferência de que trata o art. 26 da Lei 14.133/2021, tendo em vista que as hipóteses mencionadas nos incisos I e II do referido artigo carecem de regulamentação.

Exigências de habilitação

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

Habilitação jurídica

> 10.7.1. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;
>
> 10.7.2. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

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

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

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

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

Habilitação fiscal, social e trabalhista

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

10.7.8. 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.

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

10.7.10. 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;

10.7.11. Prova de inscrição no cadastro de contribuintes Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.7.12. Prova de regularidade com a Fazenda Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

10.7.13. Caso o fornecedor seja considerado isento dos tributos Municipais /Distritais 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.

Qualificação Econômico-Financeira

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

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

10.7.16. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

I - Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Naõ Circulante);

II - Solvência Geral (SG)= (Ativo Total)/(Passivo Circulante +Passivo naõ Circulante); e

III - Liquidez Corrente (LC) = (Ativo Circulante)/(Passivo Circulante).

10.7.17. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de 10% (dez por cento) do valor total estimado da parcela pertinente.

10.7.18. 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 n° 14.133, de 2021, art. 65, §1°).

10.7.19. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei no 14.133, de 2021, art. 69, §6o)

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

Qualificação Técnica

10.7.21. A empresa deve comprovar sua qualificação técnica para a prestação dos serviços em características e prazos compatíveis com o objeto desta licitação, por meio da apresentação de atestados de capacidade técnica fornecidos por pessoas jurídicas de direito público ou privado.

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

10.7.22.1. Para os itens 1, 2, 3 e 6 - Provimento de serviço de Firewall com SD-WAN em, pelo menos, 13 (treze) unidades federativas distintas no mesmo período de tempo, incluindo implantação, garantia e suporte para a solução;

10.7.22.2. Para os itens 4 e 5 – Instalação e configuração da Solução de Gerência Centralizada e Solução de Gerenciamento e Armazenamento de Logs;

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

10.7.24. Os quantitativos exigidos representam aproximadamente 50% da demanda da CGU com relação ao número de unidades da federação que serão atendidas por este Termo de Referência.

10.7.25. Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa licitante.

10.7.26. Os atestados de capacidade técnico-operacional deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente, exceto se firmado para ser executado em prazo inferior;

10.7.27 A CONTRATANTE poderá realizar diligência/visita técnica, a fim de se comprovar a veracidade do(s) Atestado(s) de Capacidade Técnica apresentado(s) pela LICITANTE, quando, poderá ser requerida cópia do(s) contrato(s), nota(s) fiscal(is) ou qualquer outro documento que comprove inequivocamente que o serviço apresentado no(s) atestado(s) foi(ram) prestado(s).

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O Valor estimado da licitação é de **R$ 9.075.999,87 (nove milhões, setenta e cinco mil novecentos e noventa e nove reais e oitenta e sete centavos)** para os 40 (quarenta meses) meses de vigência contratual.

Lote	Item	Descrição	CATSER	Qtde	Unidade	Valor estimado Mensal/item	Valor total estimado do item
1	1	**NGFW Tipo 1 - Suporte 24/7 por 36 meses - 2 equipamentos de firewall**	**27073**	36	mês	R$ 71.400,00	R$ 2.570.400,00
	2	**NGFW Tipo 2 - Suporte 24/7 por 36 meses - 13 equipamentos de firewall**	**27073**	36	mês	R$ 76.643,05	R$ 2.759.149,87
	3	**NGFW Tipo 3 - Suporte 24/7 por 36 meses - 13 equipamentos de firewall**	**27073**	36	mês	R$ 75.600,00	R$ 2.721.600,00
	4	**Solução de gerência centralizada**	**27073**	36	mês	R$ 5.475,00	R$ 197.100,00
	5	**Solução de armazenamento e gerência de logs**	**27073**	36	mês	R$ 5.600,00	R$ 201.600,00
	6	**Implantação da Solução com migração da Atual no ambiente on-premisses**	**13684**	1	unidade	R$ 85.000,00	R$ 85.000,00
	7	**Repasse de conhecimento - 60 horas**	**16837**	1	unidade	R$ 32.400,00	R$ 32.400,00
	8	**Serviço técnico especializado do fabricante**	**25631**	300	horas	R$ 1.695,83	R$ 508.750,00
						Valor total Lote/grupo:	**R$ 9.075.999,87**

Adequação Orçamentária

11.2. As despesas decorrentes da presente contrataçaõ correraõ à conta de recursos especíificos consignados no Orçamento Geral da Uniaõ e será atendida pela seguinte dotaçaõ:

11.2.1 Gestaõ/Unidade: 370041;

11.2.2. Fonte de Recursos: 33904013

11.2.3. Programa de Trabalho: [DTI] Sustentaçaõ das soluçoẽs de TI - Geral

(2023);

11.2.4. Elemento de Despesa: 1136120;

11.2.5. Plano Interno: 10.01.00

11.2.6 A Contratação em comento não prevê desembolso financeiro em 2023. Portanto o orçamento será solicitado apenas em 2024.

11.3. A dotaçaõ relativa aos exercícios financeiros subsequentes será indicada após aprovaçaõ da Lei Orçamentária respectiva e liberaçaõ dos créditos correspondentes, mediante apostilamento.

Cronograma Físico Financeiro

11.8. Essa contratação não implicará gasto financeiro em 2023. Portanto, o cronograma abaixo prevê gasto apenas em 2024.

11.9. Segue abaixo a estimativa de gasto anual do contrato.

Item	Descrição	Qtde	Und	Valor Mensal /item	2024	2025	2026	2027
1	**NGFW Tipo 1 - Suporte 24/7 por 36 meses - 2 equipamentos de firewall**	36	mês	R$ 71.400,00	R$ 571.200,00	R$856.800,00	R$ 856.800,00	R$ 285.600,00
2	**NGFW Tipo 2 - Suporte 24/7 por 36 meses - 13 equipamentos de firewall**	36	mês	R$ 76.643,05	R$ 613.144,42	R$ 919.716,62	R$919.716,62	R$ 306.572,21
3	**NGFW Tipo 3 - Suporte 24/7 por 36 meses - 13 equipamentos de firewall**	36	mês	R$ 75.600,00	R$ 604.800,00	R$ 907.200,00	R$ 907.200,00	R$302.400,00
4	**Solução de gerência centralizada**	36	mês	R$ 5.475,00	R$ 43.800,00	R$ 65.700,00	R$ 65.700,00	R$ 21.900,00
5	**Solução de armazenamento e gerência de logs**	36	mês	R$ 5.600,00	R$ 44.800,00	R$ 67.200,00	R$ 67.200,00	R$ 22.400,00
6	**Implantação da Solução com migração da Atual no ambiente on-premisses**	1	Unid	R$ 85.000,00	R$ 85.000,00	R$ -	R$ -	R$ -
7	**Repasse de conhecimento - 60 horas**	1	unid	R$ 32.400,00	R$ 32.400,00	R$ -	R$ -	R$ -
8	**Serviço técnico especializado do fabricante**	300	horas	R4 1.695,83	R$ 169.583,33	R$ 169.583,33	R$169.583,33	R$ -
				gasto anual	**R$ 2.164.727,75**	**R$ 2.986.199,95**	**R$ 2.986.199,95**	**R$ 938.872,21**

*O Contrato possui vigência de 40 (quarenta) meses, mas os quatro meses iniciais serão para implantação da solução e portanto não haverá emissão de fatura pelo serviço prestado durante esse período. O serviço provavelmente terá o faturamento iníciado em maio/2024. Portanto, calculou-se apenas 8 meses de prestação de serviço para o ano de 2024 para os itens 1 a 5.

** Foi contabilizado apenas 4 meses para o ano de 2027, que é o restante de meses para completar os 36 de vigência.

*** Para os itens 6 e 7 a expectativa é de serem executados ainda no ano de 2024.

**** Para o item 8, a expectativa é consumir 100 horas em 2024, 100 horas em 2025, 100 horas em 2026 e zero horas em 2027.

12. DO REAJUSTE DE PREÇOS

12.1 Os preços dos itens são fixos e irreajustáveis no prazo de um ano, com data-base vinculada à data do orçamento estimado.

12.2. O objeto será contratado pelo preço ofertado, sendo reajustado anualmente de acordo com o Índice de Custos de Tecnologia da Informação ICTI, instituído pela Portaria GM/MP nº 424, de 7 de dezembro de 2017, e mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA.

12.4. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

12.5. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

12.6. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

12.7. Caso o índice estabelecido para o reajuste 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.

12.8. 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.

12.9. Conforme acórdão 1374/2006 – TCU Plenário, os reajustes poderão ocorrer por simples apostilamento, devendo ser efetivados de forma automática e de ofício, não sendo exigível prévio requerimento ou solicitação por parte da CONTRATADA.

13. DA VIGÊNCIA DO CONTRATO

13.1. O contrato vigorará por 40 (quarenta) meses, contados a partir da data da sua assinatura, sendo os itens 1(um) a 5(cinco) e o item 8(oito) podendo ser prorrogado por períodos sucessivos, limitado a 120 (cento e vinte) meses, desde que haja preços e condições mais vantajosas para a Administração, nos termos dos Art. 106 e Art. 107, da Lei nº 14.133, de 2021.

13.2. Justifica-se o período inicial superior a 12 (doze) meses, pois:

13.2.1. Por trata-se de serviço continuado, a descontinuidade antecipada do serviço causaria prejuízos diante dos custos - operacionais e financeiros - de nova contratação;

13.2.2. Esta descontinuidade poderia prejudicar os serviços fornecidos pela CGU à sociedade, no caso de indisponibilidade do serviço de firewall;

13.2.3. O serviço que se pretende contratar é essencial à segurança, manutenção, otimização e recuperação da disponibilidade do acesso, pelos usuários da CONTRATANTE, à internet, que não será descontinuado nos próximos anos, apresentando tendência para ampliação de serviços e quantidade de informações a serem disponibilizadas ao cidadão;

13.2.4. A renovação contratual a cada 12 (doze) meses gera ônus administrativo, uma vez que envolve várias áreas da casa para sua realização.

14. DA ALTERAÇÃO SUBJETIVA

14.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado; e haja a anuência expressa da Administração à continuidade do contrato.

15. DA PROPOSTA COMERCIAL PARA LICITAÇÃO

15.2. A licitante deverá apresentar, juntamente com sua proposta comercial:

15.2.1. Declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio da competitividade, conforme disposto no art 5º da Lei nº 14.133, de 2021, e em atendimento ao item 1.7 do Anexo da IN SGD/ME nº 94/2021.

15.2.2. Documentação que comprove o atendimento dos requisitos estabelecidos neste Termo de Referência, em especial os requisitos técnicos estabelecidos no Anexo I, que será composta por:

15.2.2.1. Documento(s) público(s), emitidos pelo fabricante dos equipamentos/softwares, que comprovem que eles atendem cada requisito estabelecido no Anexo I.

15.2.2.2. Documento, utilizando-se, como modelo, a planilha constante do Anexo I, indicando em que documento/página está a informação para a comprovação do respectivo atendimento.

15.2.3. Declaração de estar ciente de que a CGU possui um único CNPJ, não possui inscrição estadual e não emite nota fiscal.

16. DOS ANEXOS

ANEXO I – ESPECIFICAÇÃO TÉCNICA

ANEXO II – NÍVEIS MÍNIMOS DE SERVIÇO

ANEXO III – MODELO DE TERMO DE COMPROMISSO DE CONFIDENCIALIDADE

ANEXO IV – MODELO DE TERMO DE CIÊNICA

ANEXO V - MODELO DE ORDEM DE SERVIÇO

ANEXO I – ESPECIFICAÇÃO TÉCNICA

A licitante deverá apresentar juntamente com sua proposta comercial, comprovação de que os equipamentos propostos atendem a cada um dos requisitos especificados. Tal comprovação deverá se dar por meio de indicação de documento público (eletrônico ou impresso) e da numeração da página (ou localização no texto), por meio do qual a equipe técnica da CGU possa confirmar tais argumentos.

Na Tabela de Documentação Comprobatória de Requisitos (TDCR), deverá ser especificado o documento, e, na coluna à direita das especificações, deverá ser especificado o **ÍNDICE** do documento na TDCR e a numeração da **PÁGINA** (ou localização no texto do documento) para comprovação.

A CGU reserva-se ao direito de diligenciar, após apresentação da proposta, o fornecedor e/ou fabricante para comprovação das informações prestadas na proposta e nas tabelas.

Todos os requisitos que possuem os termos “Implementar”, “ter capacidade”, “deve permitir”, “deve possibilitar” devem ser interpretados como funcionalidades a serem atendidas pelo objeto a ser contratado independentemente do fornecimento de licenças e/ou upgrades sem custo adicional para a administração.

ITEM	ESPECIFICAÇÃO	Indice e pagina		
1	REQUISITOS COMUNS - ITENS 1, 2 e 3 (NGFW Tipos 1, 2 e 3)	item 1	item 2	item3
1.1	CARACTERÍSTICAS GERAIS	-	-	-
1.1.1	Deverá possuir garantia e suporte do fabricante 24x7 e licenças para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades durante toda a vigência do contrato;	-	-	-
1.1.2	Não serão aceitas soluções personalizadas, diferentes das oferecidas pelos fabricantes de mercado;	-	-	-
1.1.3	Os equipamentos a serem fornecidos e todos os seus componentes serão novos, de primeiro uso e estão em linha de fabricação e não há anúncio de end-of-sales e end-of-support;	-	-	-
1.1.4	Deve ser do tipo appliance físico. Não serão aceitos equipamentos do tipo servidor e sistema operacional de uso genérico ou máquina virtual;	-	-	-
1.1.5	Deve contar com funcionalidades de Next Generation Firewall (NGFW). Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, análises modernas de malware, identificação de usuários e controle granular de permissões;			
1.1.6	Deve ser próprio para montagem em rack 19”, incluindo kit do tipo trilho para adaptação, além de adaptadores para racks ou bandejas, se necessário;			
1.1.7	Deve ter no mínimo 2 (duas) fontes de alimentação. As fontes de alimentação deverão ser redundantes com chaveamento automático de tensão de entrada 110/220 VAC a 60 Hz;			

1.2	**COMPATIBILIDADE COM SOLUÇÃO DE NGFW VIRTUAL EM AMBIENTE DE NUVEM**	**-**	**-**	**-**
1.2.1	O fabricante da solução oferecida deverá possuir solução de NGFW virtual disponível para aquisição de licenciamento em marketplace da AWS;			
1.2.2	O fabricante da solução oferecida deverá possuir solução de NGFW virtual disponível para aquisição em de licenciamento marketplace da Microsoft Azure;			
1.2.3	A solução oferecida deverá ser compatível com ferramenta de gerenciamento centralizado de todas as instâncias do Firewall Virtual de Nuvem a partir de um único painel de controle ou console de administração, permitindo o monitoramento, configuração e implementação de políticas de segurança de forma unificada;			
1.3	**SD-WAN E BALANCEAMENTO DE LINK**	**-**	**-**	**-**
1.3.1	Deve suportar SD-WAN de forma nativa. Entende-se como tecnologia SD-WAN (software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em firewalls/roteadores de localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou desempenho, além da utilização de túneis VPN para comunicação entre as localidades;			
1.3.2	Deve ser integrado ao appliance de NGFW, não sendo aceito um appliance separado;			
1.3.3	Deve permitir o balanceamento de pelo menos 2 (dois) links Internet;			
1.3.4	Deve implementar balanceamento de link por hash do IP de origem e destino;			

1.3.5	Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.			
1.3.6	Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;			
1.3.7	Deve permitir a configuração de link (rota “default” estática) com a utilização de “probe” para verificar a disponibilidade do provedor. A “probe” deve permitir verificar o acesso ping, http, tcp/udp echo, dns, tcp-connect e deve considerar o link indisponível em caso de falha (ou alta latência ou alta perda);			
1.3.8	A solução deve permitir a definição de diferentes políticas de balanceamento para conjuntos de aplicações específicas (definidas com base em regras);			
1.3.9	Deve realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas;			
1.3.10	Deve monitorar latência, jitter, perda de pacote, banda ocupada ou uma combinação de todos esses itens em cada um dos links individualmente;			
1.3.11	Diversas formas de escolha do link devem estar disponíveis, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;			
1.3.12	Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;			
1.3.13	Deve suportar convergência rápida de tráfego em caso de falha em um dos			

	links. Neste caso, aceita-se que as conexões existentes sejam restabelecidas pelo(s) outro(s) link(s);			
1.3.14	Deve selecionar o melhor caminho de cada sessão com base em especificações do aplicativo e das condições de rede;			
1.4	**FUNCIONALIDADES E PROTOCOLOS**	**-**	**-**	**-**
1.4.1	Policy based routing ou policy based forwarding;			
1.4.2	Jumbo Frames;			
1.4.3	DHCP Relay;			
1.4.4	Suportar IGMP, v2 e v3;			
1.4.5	Deve suportar tanto IPv4 quanto IPv6, sendo que este último deve estar implementado de forma nativa em pilha dupla;			
1.4.6	O serviço deve permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS;			
1.4.7	Roteamento IP Multicast através do protocolo PIM nas versões 1 e 2 e nos modos “Sparse” e “Dense” (não será exigida a implementação dos dois modos de forma simultânea);			
1.4.8	OSPFv2 e OSPFv3 com suporte a autenticação de vizinhança utilizando protocolo MD5;			
1.4.9	Deve suportar o protocolo padrão da indústria VXLAN;			
1.4.10	Cliente NTP, contemplando suporte à autenticação entre os “peers”;			
1.4.11	Agente SNMP nas versões 2c e 3, com suporte a MIB-II, possibilitando acesso de leitura com restrição dos endereços que podem efetuar consultas SNMP;			
1.4.12	Protocolo de coleta de informações de fluxos que circulam pelo equipamento,			

	como Netflow, sFlow, IPFIX ou similar, contemplando no mínimo as seguintes informações:			
1.4.12.1	IP de origem/destino;			
1.4.12.2	Parâmetro “protocol type” do cabeçalho IP;			
1.4.12.3	Porta TCP/UDP de origem/destino;			
1.4.12.4	Interface do equipamento em que o tráfego foi identificado.			
1.5	**NAT**	**-**	**-**	**-**
1.5.1	Deverá suportar os seguintes tipos de NAT:	**-**	**-**	**-**
1.5.1.1.	NAT dinâmico (Many-to-1);			
1.5.1.2	NAT dinâmico (Many-to-Many);			
1.5.1.3	NAT estático (1-to-1);			
1.5.1.4	NAT estático (Many-to-Many);			
1.5.1.5	NAT estático bidirecional 1-to-1;			
1.5.1.6	NAT64;			
1.5.1.7	Tradução de porta (PAT);			
1.5.1.8	NAT de origem;			
1.5.1.9	NAT de destino;			
1.5.1.10	NAT de origem e NAT de destino simultaneamente.			
1.6	**BGP**	**-**	**-**	**-**
1.6.1.	O serviço deverá ser fornecido com suporte a MP-BGP, ou seja, encaminhamento de tráfego IPv4 e IPv6;			
1.6.2	Implementar RFC 4271 BGPv4;			
1.6.3	Implementar RFC 1997 Communities and Attributes;			
1.6.4	Implementar RFC 4360 BGP Extended Communities Attribute;			
1.6.5	Implementar RFC 2918 Route Refresh Capability;			
1.6.6	Implementar RFC 2385 BGP Session Protection via TCP MD5;			
1.6.7	Implementar Generalized TTL Security Mechanism (GTSM);			

1.6.8	Implementar RFC 4893 BGP Support for Four-octet AS Number Space;			
1.6.9	Implementar Outbound Route Filtering Capability for BGP-4;			
1.6.10	Implementar RFC 2858 Multiprotocol Extensions for BGP-4;			
1.6.11	Implementar RFC 4724 Graceful Restart Mechanism for BGP;			
1.6.12	Implementar definição de políticas de controle dos anúncios BGP;			
1.6.13	Implementar aplicação de expressões regulares para filtragem de anúncios;			
1.7	**QoS (QUALIDADE DE SERVIÇO)**	**-**	**-**	**-**
1.7.1	Deve ter a capacidade de limitar o tráfego de dados por políticas de máxima largura de banda, tanto de áudio como de vídeo streaming;			
1.7.2	Deve suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários do LDAP/AD, domínio e categorias de URL, interface de origem /destino, portas TCP/UDP e aplicações de camada 7 (as mesmas disponíveis na função de NGFW);			
1.7.3	Deve permitir agendar intervalos de dias da semana e horários para o funcionamento das políticas de shaping /QoS;			
1.7.4	Deve possibilitar a definição de bandas distintas para download e upload das políticas de shaping/QoS;			
1.7.5	Deve suportar priorização de protocolos de voz e vídeo como H.323, SIP, SCCP, MGCP e aplicações como Teams;			
1.7.6	Deve implementar a classificação e a priorização do tráfego com o campo DSCP;			
1.7.7	Deve possibilitar a definição de tráfego com banda mínima garantida e banda máxima utilizável;			
1.7.8	Deve possibilitar a definição de fila de prioridade;			

1.7.9	Deve suportar marcação de pacotes Diffserv, inclusive por aplicação;			
1.7.10	Deve suportar modificação de valores DSCP para o Diffserv;			
1.7.11	Deve suportar priorização de tráfego usando informação de Type of Service;			
1.7.12	Deve suportar QoS (traffic-shaping) em interface agregadas ou redundantes.			
1.8	**CONTROLE DE POLÍTICA DE FIREWALL**	**-**	**-**	**-**
1.8.1	Controles de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;			
1.8.2	Controle, inspeção e descriptografia de TLS 1.3 por política para tráfego de entrada (inbound) e saída (outbound);			
1.8.3	Deve suportar offload de certificado em inspeção de conexões TLS 1.3 de entrada (inbound);			
1.8.4	Deve permitir bloquear arquivos com extensões tipicamente associadas a malwares;			
1.8.5	Suporte a objetos e regras multicast;			
1.8.6	Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;			
1.8.7	Deve ser possível criar políticas de firewall utilizando serviços de ameaças de terceiros, onde o firewall receberá uma lista de endereços IPs maliciosos, por exemplo, a qual poderá ser utilizada para bloqueio do tráfego;			
1.8.8	Suportar a criação de políticas com data de expiração.			
1.9	**CONTROLE DE APLICAÇÕES**	**-**	**-**	**-**
1.9.1	A plataforma deve suportar análise de conteúdo de aplicações em camada 7;			
1.9.2	Deve possuir a capacidade de reconhecer aplicações, independentemente de porta e protocolo;			

1.9.3	Deve ser possível a liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos;			
1.9.4	Reconhecer diversas aplicações diferentes, incluindo, mas não limitado: peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, audio, vídeo, proxy, mensageria instantânea, compartilhamento de arquivos, e-mail etc.			
1.9.5	Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independentemente de porta e protocolo;			
1.9.6	Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam comunicações criptografadas e ataques utilizando, por exemplo, a porta 443;			
1.9.7	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 decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo, por exemplo. Também deve ser possível a detecção de arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;			
1.9.8	Deve ser possível a liberação e bloqueio das aplicações (ou de suas funcionalidades) por usuário, grupo de usuários, endereço IP ou rede específica;			
1.9.9	Atualizar a base de assinaturas de aplicações automaticamente;			
	Deve ser possível adicionar controle de aplicações em todas as regras de			

1.9.10	segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;			
1.9.11	O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;			
1.9.12	Deve alertar o usuário quando uma aplicação for bloqueada;			
1.9.13	Deve possibilitar o controle customizados das aplicações como, por exemplo, restringir acesso a funcionalidades dentro de aplicações como Facebook ou Whatsapp;			
1.9.14	Deve possibilitar a diferenciação do acesso de vídeos baseadas na qualidade da resolução em plataformas de streaming, como YouTube;			
1.9.15	Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, ultrasurf, tor, etc) possuindo granularidade de controle/políticas para os mesmos;			
1.9.16	Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:			
1.9.16.1	Tecnologia utilizada nas aplicações (client-server, browser based, network protocol etc);			
1.9.16.2	Nível de risco da aplicação;			
1.9.16.3	Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda etc.			
1.10	**PREVENÇÃO DE AMEAÇAS**	**-**	**-**	**-**
1.10.1	A solução de proteção deverá possuir módulo de IPS integrado no próprio equipamento de firewall;			
1.10.2	Deve bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;			

1.10.3	Deve-se sincronizar as assinaturas de IPS quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;			
1.10.4	Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2;			
1.10.5	As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;			
1.10.6	Deve ser possível a criação de regras de exceções por IP, de origem ou de destino, das formas: geral e assinatura por assinatura;			
1.10.7	Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall, considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS;			
1.10.8	Identificar e bloquear comunicação com botnets;			
1.10.9	Deve suportar várias técnicas de prevenção, incluindo Drop (Cliente, Servidor e ambos);			
1.10.10	Deve suportar referência cruzada com CVE;			
1.10.11	Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;			
1.10.12	Deve suportar a captura de pacotes (PCAP), por assinatura de IPS;			
1.10.13	Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos. A identificação deve ser de forma automática, não sendo necessário que o			

	administrador cadastre os domínios considerados maliciosos;			
1.10.14	Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;			
1.10.15	Suportar a criação de políticas por Geolocalização, permitindo que o tráfego de determinado País/Países seja bloqueado;			
1.10.16	Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas;			
1.11	**ANÁLISE DE MALWARES MODERNOS**	**-**	**-**	**-**
1.11.1	A solução de proteção deverá possuir módulo de análise de Malwares integrado no próprio equipamento de firewall;			
1.11.2	A solução deverá utilizar algoritmos de aprendizado de máquina (IA/ML) para a análises modernas de malware;			
1.11.3	Deve possuir análise de malwares desconhecidos (dia zero);			
1.11.4	Deve ser capaz de enviar malwares não conhecidos de forma automática para análise em nuvem do Fabricante ou localmente no equipamento, onde o arquivo será executado e simulado em ambiente controlado (sandbox);			
1.11.5	Deve implementar o bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido;			
1.11.6	Deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado;			
1.11.7	Deverá gerar relatórios detalhados sobre a atividade dos arquivos analisados, incluindo registros de eventos e informações sobre as ameaças detectadas;			
1.11.8	Suportar bloqueio por tipo de arquivos;			
1.11.9	Suportar rastreamento de vírus em arquivos pdf;			
1.11.10	Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);			

1.11.11	Deve permitir a inspeção de arquivos incorporados em outros arquivos ou arquivos que tenham sua extensão alterada na tentativa de contornar sua detecção;			
1.11.12	Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;			
1.11.13	Proteção contra downloads involuntários de arquivos executáveis maliciosos.			
1.12	**IDENTIFICAÇÃO DE USUÁRIOS**	**-**	**-**	**-**
1.12.1	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem (usuários e grupos de usuários) está utilizando quais aplicações por meio da integração com serviços de diretório, Microsoft Active Directory e base de dados local;			
1.12.2	Suporte a autenticação Kerberos;			
1.12.3	Quando integrado ao Microsoft Active Directory, deve permitir identificar usuários dentro de grupos;			
1.12.4	Deve possuir suporte a identificação de múltiplos usuários conectados, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão em uso;			
1.12.5	Deve permitir a atualização da identificação de um usuário caso este mude de endereço IP e mesmo que mais de um dispositivo esteja sendo utilizado de forma simultânea, evitando a necessidade de que sejam configurados endereços fixos;			
1.12.6	O firewall deve suportar Single Sign-On (SSO) para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos a organização através dos protocolos: SAML ou OpenID Connect (OIDC).			

1.13	**FILTRO DE URLS**	**-**	**-**	**-**
1.13.1	Deve implementar a funcionalidade de filtro de URL HTTP e HTTPS;			
1.13.2	Deve implementar a funcionalidade de filtro de conteúdo HTTP e HTTPS;			
1.13.3	Deve implementar a funcionalidade de TLS Scanner;			
1.13.4	Deve ter funcionalidade de proxy transparente HTTP/HTTPS (situação em que o cliente não precisa encaminhar o tráfego para o IP do proxy e não há instalação de cliente). No modo proxy transparente o cliente acreditar estar acessando diretamente o conteúdo desejado;			
1.13.5	Deve implementar a funcionalidade de cache de dados;			
1.13.6	Deve bloquear as tentativas de acesso proibidas pela política antes que ocorra o carregamento da página solicitada, exibindo mensagem customizada para o bloqueio;			
1.13.7	Deve garantir o monitoramento do tráfego internet independente de plataforma, sistema operacional ou aplicação utilizada pelos usuários;			
1.13.8	Para prover esta funcionalidade, não deve instalar nem executar agentes, módulos ou scripts nas estações de trabalho para prover qualquer serviço. Deve ser transparente ao usuário final;			
1.13.9	**Controle de acesso à Internet**	**-**	**-**	**-**
1.13.9.1	Regras de acesso à Internet devem se basear tanto na requisição quanto na resposta HTTP;			
1.13.9.2	Deve permitir a criação de regras baseadas em horário do dia;			
1.13.9.3	Deve possuir controle de downloads /uploads de arquivos pelo nome, tipo ou extensão do arquivo;			
1.13.9.4	Deve possuir controle de acesso à Internet por domínio, exemplo: gov.br, org.br;			

1.13.9.5	Deve possuir controle de acesso à Internet por categorias de sites web;			
1.13.9.6	Deve possuir controle para bloqueio de acesso à Internet por lista de sites web proibidos (blacklist) customizável;			
1.13.9.7	Deve possuir controle de acesso à Internet por lista de sites web permitidos (whitelist) customizável;			
1.13.9.8	Deve possuir mecanismo automático para detecção e bloqueio em tempo real de tráfego (inbound/outbound) originado por malwares;			
1.13.9.9	O serviço deve possuir mecanismo automático para detecção de tráfego tunelado;			
1.13.9.10	Deve permitir que as páginas de erro e bloqueio sejam customizáveis;			
1.13.9.11	Deve possuir compatibilidade com filtros de busca segura (safe-search filters), oferecidos por sites web de busca;			
1.13.9.12	Deve permitir a definição e aplicação das regras por meio de expressões regulares;			
1.13.9.13	Deve permitir a liberação/bloqueio de componentes específicos de sites de redes sociais, tais como chat e comentários do site facebook.com ou postagem no site twitter.com;			
1.13.10	**Categorização de sites web**	**-**	**-**	**-**
1.13.10.1	Deve conter base de URLs cadastradas com categorias previamente definidas e possibilidade de criação de novas categorias personalizadas;			
1.13.10.1.1	Deve possuir no mínimo as seguintes categorias (ou similares): pornografia, nudez, sites maliciosos, webmail, blog /fotolog, jogos, hacking, racismo, comunidades virtuais, radio e tv, streaming, instant messaging, chat, sites de download, storage online, P2P, medias sociais, sites maliciosos e acesso remoto;			
1.13.10.1.2	Deve permitir a classificação /categorização de sites de acordo com o			

	assunto;			
1.13.10.1.3	Deve possibilitar que URLs não cadastradas possam ser enviadas ao fabricante para a devida categorização;			
1.13.10.1.4	Deve permitir à CONTRATANTE reclassificar, a seu critério, os registros de site web que julgar necessários.			
1.13.11	Atualização da base de sites	**-**	**-**	**-**
1.13.11.1	Durante o período de prestação do serviço a base de sites web deve ser atualizada automaticamente pela solução, via Internet, com periodicidade de atualização customizável;			
1.13.11.2	A atualização da base de sites web deve transcorrer de forma transparente, sem comprometer a execução dos serviços;			
1.13.11.3	A ausência de atualização da base de sites web, por qualquer motivo, não deve interromper nem comprometer funcionalidades da solução;			
1.13.11.4	Durante o período de prestação do serviço, os sites webs devem ser atualizados, sempre na categoria que reflita o seu conteúdo mais recente, ou seja, em caso de modificação, deve ser reclassificado para a categoria pertinente;			
1.13.11.5	Durante o período de prestação do serviço, sites web de phishing, spyware ou que tenham sido usados para hospedar códigos maliciosos, devem retornar à categoria original depois de “descontaminados”;			
1.14	**VPN**	**-**	**-**	**-**
1.14.1	Deve implementar VPN IPSec com capacidade de implementar túneis site-to-site do tipo hub-and-spoke;			
1.14.2	Deve permitir o estabelecimento do túnel utilizando uma “chave secreta” ou certificados digitais;			
1.14.3	Deve implementar IKEv1 e IKEv2;			
1.14.4	Deve oferecer suporte pelo menos aos seguintes algoritmos de criptografia: AES-128, AES-192 e AES-256;			

1.14.5	Deve oferecer suporte pelo menos aos seguintes algoritmos de autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512;			
1.14.6	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis TLS;			

2	**REQUISITOS ESPECÍFICOS – ITEM 1 – NGFW TIPO 1 (SEDE/DF)**	**Índice e Página**
2.1	**DESEMPENHO**	-
2.1.1	Deve suportar, no mínimo, 12.5 (doze ponto cinco) Gbps com as funcionalidades de Threat Protection/Prevention Throughput (firewall, controle de aplicação, IPS e antimalware) habilitadas e atuantes ou, no mínimo, 22 (vinte e dois) Gbps com as funcionalidades de NGFW (firewall, controle de aplicação e IPS) habilitadas e atuantes;	
2.1.2	Deve suportar, no mínimo, 3 (três) milhões de sessões concorrentes;	
2.1.3	Deve suportar, no mínimo, 250.000 (duzentos e cinquenta mil) novas sessões por segundo;	
1.1.4	Além das interfaces utilizadas para gerência e para funcionamento do cluster deve possuir pelo menos 4 (quatro) interfaces GigabitEthernet (10 /100/1000Base-T);	
2.1.5	Deve possuir 4 (quatro) interfaces 1000Base-SX;	

1.1.6	Deve possuir 4 (quatro) interfaces 10Gbase-SR;	
2.1.7	Deve possuir 2 (duas) interfaces 25Gbase-SR;	
2.1.8	Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação.	-
2.2	**SD-WAN E BALANCEAMENTO DE LINK**	-
2.2.1	Deve permitir a criação de 2 (dois) túneis VPN IPSec com cada unidade regional;	
2.3	**ALTA DISPONIBILIDADE E BALANCEAMENTO DE CARGA**	-
2.3.1	Deve possibilitar que 2 equipamentos formem um cluster Ativo/Ativo e Ativo/Passivo;	
2.3.1.1	Em caso de falha em um dos nós, o remanescente deverá assumir o controle automaticamente;	
2.3.2	O modo de alta disponibilidade deve sincronizar:	-
2.3.2.1	a) todas as sessões;	
2.3.2.2	b) certificados descriptografados;	
2.3.2.3	c) todas as associações de segurança das VPNs;	
1.3.2.4	d) todas as assinaturas de Antimalware, Aplicações Web e IPS;	
2.3.2.5	e) todas as configurações.	
2.3.3	Deve realizar monitoramento de falhas de links;	
2.3.4	Deve suportar mais de dois membros no cluster, para melhor desempenho ou em caso de crescimento da rede;	
2.3.5	Deve suportar fazer port-aggregation de interfaces no firewall suportando os protocolos 802.3ad e XOR para aumento de throughput e	

	alta disponibilidade de interfaces;	
2.4	**ACESSO REMOTO/VPN**	
2.4.1	Deve implementar VPN TLS com capacidade de implementar client-to-site, para no mínimo, 92 usuários simultâneos;	
2.4.2	**A VPN TLS cliente-to-site**	-
2.4.2.1	Deverá suportar autenticação por Microsoft Active Directory (AD) ou Azure Active Directory (AAD), certificado digital e base de usuários local;	
2.4.2.1.1	Deverá possuir configuração para imposição de segundo fator de autenticação (2FA) com aplicativo de celular no modo Push Notification ou One Time Password (OTP);	
2.4.2.2	O usuário deverá realizar a conexão à VPN TLS por meio de agente instalado no sistema operacional do equipamento;	
2.4.2.3	Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuários e grupos do AD;	
2.4.2.4	Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;	
2.4.2.5	Deve possuir atribuição de DNS nos clientes remotos de VPN;	
2.4.2.6	Deve suportar a leitura e verificação de CRL (certificate revocation list);	
2.4.3	**O agente da VPN TLS**	-
2.4.3.1	Deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;	
2.4.3.2	Deve ser compatível com pelo menos: Windows 10, Windows 11, MacOS X, GNU/Linux;	
2.4.3.3	Deve também suportar dispositivos móveis: iOS (Apple) e Android;	
2.4.3.4	Deve possuir mecanismos de checagem de conformidade do dispositivo remoto, como, no mínimo, se há cliente de antivírus instalado.	

3	**REQUISITOS ESPECÍFICOS – ITEM 2 - NGFW TIPO 2 (REGIONAIS)**	**Índice e Página**
3.1	**DESEMPENHO**	-
3.1.1	Deve suportar, no mínimo, 2.2 (dois ponto dois) Gbps com as funcionalidades de Threat Protection /Prevention Throughput (firewall, controle de aplicação, IPS e antimalware) habilitadas e atuantes ou, no mínimo, 3.9 (três ponto nove) Gbps com as funcionalidades de NGFW (firewall, controle de aplicação e IPS) habilitadas e atuantes;	
3.1.2	Deve suportar, no mínimo, 1 (um) milhão de sessões concorrentes;	
3.1.3	Deve suportar, no mínimo, 45.000 (quarenta e cinco mil) novas sessões por segundo;	
3.1.4	Além das interfaces utilizadas para os links internet, deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T).	
3.1.5	Deve possuir pelo menos 2 (duas) interfaces 1000base-SX.	
3.1.6	Deve possuir pelo menos 2 (duas) interfaces 10Gbase-SR.	
3.1.7	Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação.	
3.1.8	**SD-WAN E BALANCEAMENTO DE LINK**	-

3.1.9	Deve permitir a criação de túneis VPN IPSec com os firewalls de todas as outras unidades regionais de forma estática (full-mesh) ou dinâmica;	
3.1.10	Deve permitir a criação de 2 (dois) túneis VPN IPSec com a sede (DF).	

4	**REQUISITOS ESPECÍFICOS DE NGFW – TIPO 3 (REGIONAIS)**	**Índice e Página**
4.1	**DESEMPENHO**	-
4.1.1	Deve suportar, no mínimo, 1.8 (um ponto oito) Gbps com as funcionalidades de Threat Protection /Prevention Throughput (firewall, controle de aplicação, IPS e antimalware) habilitadas e atuantes ou, no mínimo, 3.2 (três ponto dois) Gbps com as funcionalidades de NGFW (firewall, controle de aplicação e IPS) habilitadas e atuantes;	
4.1.2	Deve suportar, no mínimo, 1 (um) milhão de sessões concorrentes;	
4.1.3	Deve suportar, no mínimo, 45.000 (quarenta e cinco mil) novas sessões por segundo;	
4.1.4	Além das interfaces utilizadas para os links internet, deve possuir pelo menos 2 (duas) interfaces GigabitEthernet (10/100/1000Base-T).	

4.1.5	Deve possuir pelo menos 2 (duas) interfaces 1000base-SX.	
4.1.6	Deve possuir pelo menos 2 (duas) interfaces 10Gbase-SR.	
4.1.7	Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação.	
4.1.8	**SD-WAN E BALANCEAMENTO DE LINK**	-
4.1.9	Deve permitir a criação de túneis VPN IPSec com os firewalls de todas as outras unidades regionais de forma estática (full-mesh) ou dinâmica;	
4.1.10	Deve permitir a criação de 2 (dois) túneis VPN IPSec com a sede (DF).	

5	**SOLUÇÃO DE GERÊNCIA CENTRALIZADA – ITEM 5**	**Índice e Página**
5.1	**REQUISITOS GERAIS**	-
5.1.1		

	Da Infraestrutura	-
5.1.1.1	Deverá prover solução de gerência centralizada, através de appliance virtual, para gerência dos equipamentos de NGFW;	
5.1.1.1.1	Por solução de gerência centralizada, entende-se as licenças de software necessárias para esta funcionalidade;	-
5.1.1.1.2	Deverá ser necessariamente solução do mesmo fabricante dos NGFW ofertados, não serão aceitas soluções desenvolvidas ou customizadas de outros fornecedores;	-
5.1.1.1.3	O appliance virtual da solução será implantado utilizando a infraestrutura, processamento e armazenamento da CONTRATANTE;	-
5.1.1.2	Deverá possuir garantia com suporte 24x7 e licenças para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades durante toda a vigência do contrato;	-
5.1.1.3	Deverá ser baseada em appliance ou em servidor virtual compatível com a plataforma de virtualização VMware Vsphere ESXi 7;	

5.1.1.4	Deverá fornecer todo o licenciamento da solução com capacidade para gerenciar, no mínimo, 37 equipamentos de NGFW;	-
5.1.2	**Das Compatibilidades com solução de nuvem**	-
5.1.2.1	A solução de gerência centralizada deverá ser compatível e possuir licenciamento para gerência de NGFW Virtuais instalados em nuvem da AWS ou Microsoft Azure;	-
5.1.3	**Das Funcionalidades**	-
5.1.3.1	Deverá ser acessível por portal Web e command line interface (CLI);	
5.1.3.2	Deverá suportar criptografia em todo o tráfego de rede para comunicação, sempre utilizando protocolos seguros como HTTPS e SSH.	
5.1.3.3	Deve possuir integração da autenticação com Microsoft Active Directory (AD) ou Azure Active Directory (AAD);	
5.1.3.4	Deverá possuir Segundo Fator de Autenticação (2FA) com o uso de aplicativo de celular com Push Notification ou One Time Password (OTP);	
	Deverá permitir aplicar políticas para o uso de senhas de usuários locais da plataforma, como	

5.1.3.5	tempo de expiração, tamanho mínimo e caracteres exigidos;	
5.1.3.6	Deve permitir acesso simultâneo à administração;	
5.1.3.7	Deve permitir a geração de logs de auditoria com detalhes de configurações efetuadas, com no mínimo o usuário que efetuou a alteração e seu horário;	
5.1.3.8	Deve suportar à 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;	
5.1.3.9	Deve suportar backup das configurações com versionamento e aplicação de rollback para uma versão anterior;	
5.1.3.10	Deve suportar a visualização e comparação das configurações atuais de um equipamento com configurações anteriores;	
5.1.3.11	Deve suportar a atualização de sistema operacional dos equipamentos bem como o rollback em caso de falha;	
5.1.3.12	Deve possibilitar a criação e administração de	

	políticas de firewall e controle de aplicação;	
5.1.3.13	Deve possibilitar a criação e administração de políticas de IPS e Antimalware;	
5.1.3.14	Deve possibilitar a criação e administração de políticas de Filtro de URL;	
5.1.3.15	Deve possibilitar a busca de objetos como: regras, hosts, redes, aplicações;	
5.1.3.16	Deve permitir a criação de grupos de dispositivos com a possibilidade de aplicar a mesma política em vários dispositivos de forma simultânea;	
5.1.3.17	Deve possuir mecanismo de validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);	
5.1.3.18	A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos equipamentos;	
5.1.3.19	Deve permitir a exibição de as informações do sistema, como licenças, memória, disco rígido, uso da CPU, total de logs diários recebidos, alertas do sistema, entre outros;	
5.1.3.20	Deve possuir suporte para SNMP versão 2 e 3;	

5.1.3.21	Deve permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTPS e SSH.	

6	**SOLUÇÃO DE GERÊNCIA E ARMAZENAMENTO DE LOGS – ITEM 6**	**Índice e Página**
6.1	**REQUISITOS GERAIS**	-
6.1.1	**Da Infraestrutura**	-
6.1.1.1	Deverá prover solução de gerência e armazenamento de logs, através de appliance virtual, para coleta e armazenamento de logs dos equipamentos de NGFW;	
6.1.1.1.1	Por solução de gerência centralizada, entende-se as licenças de software necessárias para esta funcionalidade;	-
6.1.1.1.2	Deverá ser necessariamente solução do mesmo fabricante dos NGFW ofertados, não serão aceitas soluções desenvolvidas ou customizadas de outros fornecedores;	-
6.1.1.1.3	O appliance virtual da solução será implantado utilizando a infraestrutura, processamento e armazenamento da CONTRATANTE;	-
6.1.1.2	Deverá possuir garantia com suporte 24x7 e licenças para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades durante toda a vigência do contrato;	-

6.1.1.3	Deverá ser baseada em appliance ou em servidor virtual compatível com a plataforma de virtualização VMware Vsphere ESXi 7;	
6.1.1.4	Deverá fornecer todo o licenciamento da solução com capacidade para gerenciar, no mínimo, 37 equipamentos de NGFW;	-
6.1.1.5	Deverá possuir todo o licenciamento da solução com suporte e garantia, vigentes no fabricante da solução durante toda a execução contratual, para atendimento da capacidade de 45GB de logs/dia;	-
6.1.2	**Das Compatibilidades com solução de nuvem**	-
6.1.2.1	A solução de gerenciamento e armazenamento de logs deverá ser compatível e possuir licenciamento para recebimento de logs de NGFW Virtuais instalados em nuvem da AWS ou Microsoft Azure;	-
6.1.3	**Das Funcionalidades**	-
6.1.3.1	Deverá ser acessível por portal Web;	
6.1.3.2	Deverá suportar criptografia em todo o tráfego de rede para comunicação, sempre utilizando protocolos seguros como HTTPS ou SFTP;	
6.1.3.3	Deve possuir integração da autenticação com Microsoft Active Directory (AD) ou Azure Active Directory (AAD);	

6.1.3.4	Deverá possuir Segundo Fator de Autenticação (2FA) com o uso de aplicativo de celular com Push Notification ou One Time Password (OTP);	
6.1.3.5	Deverá permitir aplicar políticas para o uso de senhas de usuários locais da plataforma, como tempo de expiração, tamanho mínimo e caracteres exigidos;	
6.1.3.6	Deve permitir acesso simultâneo à administração;	
6.1.3.7	Deve permitir a geração de logs de auditoria com detalhes de configurações efetuadas, com no mínimo o usuário que efetuou a alteração e seu horário;	
6.1.3.8	Deve suportar à 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;	
6.1.3.9	Deve permitir o envio automático dos logs para um servidor SFTP ou Syslog externo a solução;	
6.1.3.10	Deve monitorar e analisar o tráfego dos equipamentos e demonstrar informações quanto a seu uso, como quantidade de largura de banda utilizada e diferentes aplicativos;	
6.1.3.11	Deverá possuir relatórios predefinidos sobre identificações de possíveis ameaças;	
	Deve ter a capacidade de exportar relatórios nos	

6.1.3.12	formatos: HTML ou PDF;	
6.1.3.13	Permitir a personalização de qualquer relatório pré-estabelecido pela solução para adotá-lo de acordo com suas necessidades;	
6.1.3.14	Deve permitir que os relatórios sejam enviados por e-mail para um destinatário específico;	
6.1.3.15	Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;	
6.1.3.16	Deve permitir exportar os logs no formato CSV;	
6.1.3.17	Deve permitir a exibição de logs recebidos, por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;	
6.1.3.18	Permitir a exibição da taxa de geração de logs de cada dispositivo gerenciado;	
6.1.3.19	Gerar alertas automáticos por e-mail com base em eventos especiais em logs, gravidade do evento, entre outros;	
6.1.3.20	Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.	

7	**IMPLANTAÇÃO DA SOLUÇÃO COM A MIGRAÇÃO DA SOLUÇÃO ATUAL – ITEM 7**	**Índice e Página**
7.1	**REQUISITOS GERAIS**	-
7.1.1	Deverá envolver todas as atividades necessárias para a completa implantação dos itens 1, 2, 3, 4 e	

	5 com o atendimento das demandas apresentadas pela CONTRATANTE;	-
7.1.2	A CONTRATADA deverá indicar um gerente de projetos, detentor de diploma de nível superior em qualquer área, com experiência profissional mínima de 2 anos em gerenciamento de projetos e certificação Project Management Professional (PMP) ou similares. Este profissional será responsável pelo planejamento e acompanhamento de todas as atividades, controle de prazos, esforço, elaboração de relatórios de posicionamento executivo, indicadores do projeto;	-
7.1.3	A CONTRATADA deverá indicar um responsável técnico, detentor de diploma de nível superior em áreas afins de Tecnologia da Informação, com certificação avançada ou administrador ou profissional oficial do fabricante na solução de firewall ofertada e experiência profissional mínima de 3 anos em soluções de firewall. Este profissional será responsável por conduzir e acompanhar todas as atividades técnicas de planejamento e operacionais durante as atividades de implantação e migração da solução atual;	-
	Deve ser desenvolvido o Plano de Implantação e Migração da Solução atual com, no mínimo, os	

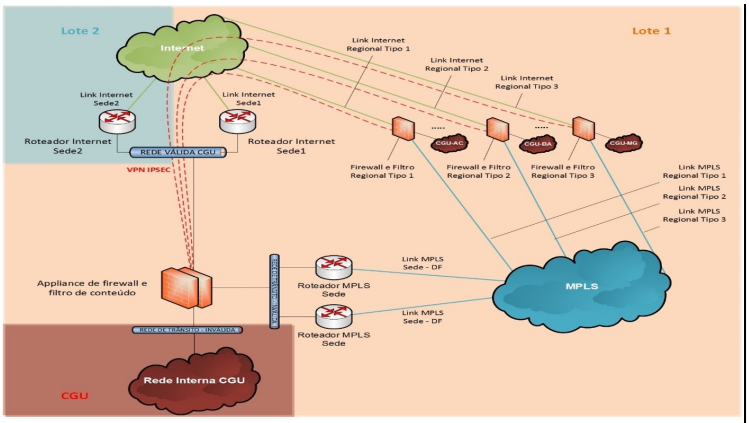
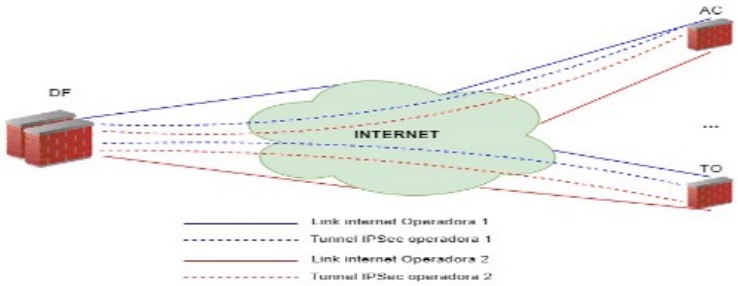
7.1.4	seguintes conteúdos: · Levantamento da Solução atual, contendo: Topologia Física, Lógica, funcionalidades habilitadas, configurações, redes, regras e todas as demais informações necessárias que devam ser levantadas para migração completa da solução; · Plano com a melhor abordagem para migração do Levantamento da Solução atual para a nova solução; · Plano de Autenticação e Roles de Acesso: definições das Formas de Autenticação da solução para implementação de 2FA e para autenticação de clientes SSO; e roles de acessos compartilhados Administrador Total, Administrador Redes, Administrador Segurança, etc; · Plano de implantação da Solução de Gerenciamento Centralizado (item 4); · Plano de implantação das Configurações para integração do envio de logs para a Solução de Armazenamento e Gerenciamento de Logs (item 5); · Plano de implantação de novas funcionalidades e sugestões de melhoria para segurança: Deep Inspection, IPS, Antimalware, Sandbox, etc.; · Plano de testes: teste de alta disponibilidade etc.; · Cronograma completo com os prazos de todas as atividades do projeto desde a entrega dos equipamentos, instalação e configuração iniciais dos equipamentos para gerenciamento remoto e todas as demais atividades necessárias para da migração para nova solução;	-	

7.1.5	O serviço de implantação envolverá todas as atividades de instalações de equipamentos, configurações, migrações, personalizações para completo atendimento das demandas apresentadas pela CONTRATANTE;	-
7.1.6	Os serviços de implantação serão realizados presencialmente, nas dependências da Sede CONTRATANTE (Brasília/DF), com disponibilidade da utilização de equipamentos de desktops, acesso à internet e apoio operacional terceirizado remoto da CONTRATANTE 24 x 7, caso necessárias manutenções fora do horário de expediente;	-
7.1.7	Após a entrega dos equipamentos nas Regionais, a instalação no rack e a configuração inicial dos equipamentos para ativação do gerenciamento remoto poderão ser realizados de forma remota pela CONTRATADA, desde que promova a devida orientação do técnico local da CONTRATANTE na Regional, com disponibilidade em dias e horários de expediente;	-
	Com o equipamento instalado e a gerência remota ativa, a migração da solução atual será dividida em 3 etapas: I) migração da Sede (Brasília/DF), com participação presencial por parte da CONTRATADA na configuração avançada de	

7.1.8	todos os equipamentos físicos e software de gerência centralizada; II) migração com participação presencial por parte da CONTRATADA, em pelo menos 3 Regionais, as quais serão definidas em momento oportuno; III) migração das regionais restantes, com acompanhamento remoto por parte da CONTRATADA e orientação do técnico local da CONTRATANTE.	-
7.1.9	Todos os componentes firmwares dos equipamentos e componentes de softwares da solução deverão ser entregues atualizados e com todos os patches de segurança aplicados.	-
7.1.10	Deverá ser fornecido, ao final do serviço de implantação e migração da solução atual, a documentação passo-a-passo de toda a implantação (as-built), com, no mínimo, os seguintes conteúdos: · Arquitetura Física e Lógica; · Integração da autenticação das soluções de gerenciamento centralizada e VPN com AD ou AAD e configurações das autenticações com 2FA; · Roles e grupos de administração; · Passo-a-passo das funcionalidades implantadas; · Passo-a-passo de como executar a migração	-

	da arquitetura da antiga para a nova arquitetura da rede WAN, conforme especificado no item 7.2; · Acesso, adição de novos equipamentos e criação de políticas na Solução de Gerenciamento centralizado (item 4); · Acesso, busca de logs e geração de relatórios na Solução de Armazenamento e Gerenciamento de Logs (item 5).	
7.2	**INFORMAÇÕES ADICIONAIS - TOPOLOGIAS DA CONTRANTATE**	-
7.2.1	A atual solução de firewall da CONTRATANTE é provida pelo fabricante Fortinet. Segue abaixo a correspondência entre os equipamentos a serem migrados: · Item 1 – 2 (dois) NGFW – Tipo 1: irão substituir os atuais 2 (dois) FortiGate-1200D, localizados no Datacenter do SERPRO na Sede (Brasília/DF); · Item 2 – 13 (treze) NGFW – Tipo 2: irão substituir os atuais 13 (treze) FortiGates-81E/101E, localizados nas unidades da Federação: BA, CE, GO, MA, MG, PA, PB, PE, PR, RJ, RS, SC e SP. · Item 3 – 13 (treze) NGFW – Tipo 3: irão substituir os atuais 13 (treze) FortiGates-81E/101E, localizados nas unidades da Federação: AC, AL, AM, AP, ES, MS, MT, PI, RN, RO, RR, SE e TO.	-
	A unidade da Sede (Brasília/DF) sai para a internet	

7.2.2	por meio de 2 (dois) links internet de operadoras distintas. Portanto, as duas unidades dos equipamentos NGFW – Tipo 1 devem ser configurados para operar como um cluster, apresentando-se como uma única entidade de firewall para fins de gerenciamento.	-
7.2.3	No momento presente, cada unidade regional apresenta 1 (um) link internet e 1 (link) MPLS. Assim, os equipamentos NGFW - Tipo 2 serão instalados nas 13 (treze) maiores unidades regionais da CONTRATANTE, enquanto os equipamentos NGFW – Tipo 3 serão instalados nas 13 (treze) menores unidades regionais da CONTRATANTE, conforme subitens abaixo.	-
7.2.4	Durante a fase de implantação, a CONTRATANTE estará em processo de modernização da sua rede WAN. Onde em sua nova topologia, os links MPLS, que conectam as unidades Regionais à Sede, serão substituídos por um segundo link de internet. Com essa mudança, cada unidade regional terá um total de dois links de internet. Adicionalmente, as unidades regionais devem se ligar à unidade central por meio de 2 (dois) túneis IPsec, sendo um túnel por cada link de internet.	-
	A representação lógica da antiga topologia da RedeWAN é representada na figura a abaixo.	

7.2.4.1		-
7.2.4.2	A representação lógica da nova topologia da Rede Wan está representada na figura abaixo. 	-
7.2.5	Devido à interdependência entre este projeto e o projeto de atualização da rede WAN da CONTRATANTE, e considerando que ambos serão implantados em intervalos próximos, a CONTRATADA deverá estar preparada para implementar a solução em conformidade com ambas as topologias de rede, tanto a atual quanto a nova planejada.	-

8	**REPASSE DE CONHECIMENTO – ITEM 7**	**Índice e Página**
8.1	**REQUISITOS GERAIS**	-

8.1.1	O repasse de conhecimento visará ao máximo a transferência de conhecimento necessário à equipe da CGU para a correta instalação, configuração, operação e administração de todos os produtos ofertados.	-
8.1.2	O repasse deverá possuir carga horária de, no mínimo, 60 (sessenta) horas, e será ministrado em dias úteis, em períodos de até 4 (quatro) horas diárias, de forma a não prejudicar o andamento de outras atividades da CONTRATANTE;	-
8.1.3	O repasse de conhecimento será executado na modalidade Remota para um público de até 8 (oito) alunos e 8 (oito) ouvintes;	-
8.1.3.1	O conteúdo do repasse deverá ser gravado pela CONTRATADA que irá disponibilizar os arquivos para download da CONTRATANTE;	-

8.1.4	O repasse de conhecimento deverá ser do tipo Hands-On;	
8.1.4.1	Deverá haver laboratório com pelo menos 1 (um) PoD (Point of Delivery), por aluno. O laboratório deve utilizar equipamentos do mesmo fabricante com as mesmas funcionalidades e interface/sintaxe que aqueles ofertados para esta contratação;	-
8.1.5	O instrutor do Repasse de Conhecimento deverá possuir certificação avançada ou administrador ou profissional oficial do fabricante na solução de firewall. A indicação do profissional e a comprovação da sua certificação deverão ser entregues à CONTRATANTE em até 10 dias úteis antes do início do Repasse de Conhecimento;	-
	O conteúdo do repasse de conhecimentos deverá comtemplar todas as soluções contratadas para os itens 1, 2, 3, 4 e 5 com, no mínimo, os seguintes tópicos: · Visão geral da solução; · Configurações físicas e lógicas dos equipamentos; · Tráfego de redes: NAT, QoS, Traffic Shaping, Protocolos de roteamento, Configuração de BGP, Configuração do SD-WAN (incluindo balanceamento entre os links), VPN site-to-site, túneis IPSec, Testes de verificação e saúde dos links;	

8.1.6	· Funcionalidades de segurança: IPS, Controle de aplicação, Antimalware, Sandbox, Identificação de usuário, Filtro de conteúdo web; · VPN client-to-site: configurações de 2FA, habilitação de políticas de compliance de dispositivos; · Solução de Gerenciamento Centralizada: atualização de versão do produto, aplicação de patches de segurança; · Solução de Armazenamento e Gerência de Logs: busca de logs, geração e personalização de relatórios; · Monitoramento e Troubleshooting de todas as ferramentas; · Instruções sobre a migração dos firewalls das regionais da topologia antiga (1 link internet e 1 MPLS) para a topologia futura (2 links internet).	-
8.1.7	O repasse de conhecimento deverá ser ministrado em língua portuguesa.	-
8.1.8	A CONTRATADA deverá fornecer certificado de participação, contendo no mínimo as informações abaixo: · Nome completo do participante; · Data de início e fim do Repasse de conhecimento; · Carga horária total; · Nome das soluções do repasse de conhecimento.	-

9	**SERVIÇO TÉCNICO ESPECIALIZADO DO FABRICANTE – ITEM 8**	**Índice e Página**
9.1	**REQUISITOS GERAIS**	-

9.1.1	A utilização do serviço técnico especializado do fabricante visa a utilização de serviços proativos para planejamento e implantação de futuros projetos de novas arquiteturas, produtos ou funcionalidades para as soluções contratadas ou novas soluções, do mesmo fabricante, que a CONTRATANTE possa vir a adquirir on-premises ou em nuvem (AWS ou Microsoft Azure);	-
9.1.2	A CONTRATANTE, a qualquer tempo da vigência do contrato e previamente à abertura da Ordem de Serviço (OS), poderá contactar a CONTRATADA, em conjunto com o serviço técnico especializado do fabricante da solução, para planejar um escopo e estimar a quantidade de horas necessárias para a sua execução;	-
9.1.3	O serviço técnico deverá ser executado por profissional técnico do fabricante, o qual deverá possuir alto conhecimento técnico com nível de arquiteto, engenheiro ou cargo similar e ser especializado no tema de escopo a ser abordado pela CONTRATANTE.	-
9.1.4	O serviço técnico de suporte será executado de forma remota em conjunto com a CONTRATANTE, preferencialmente em dias úteis e em horário comercial.	-

ANEXO II – NÍVEIS MÍNIMOS DE SERVIÇO

1. Nível Mínimo de Serviço (NMS)

1.1. O Nível Mínimo de Serviço define os termos e as condições sob as quais a CONTRATADA deverá prover o serviço de firewall com a garantia e suporte elencadas no Termo de Referência;

1.2. O serviço de garantia e suporte técnico deverá ser prestado, remotamente quando possível e pessoalmente, quando

necessário, nos locais de instalação dos equipamentos;
1.3. Deverá ser disponibilizado no portal de atendimento área de consulta do chamado, incluindo hora de abertura e fechamento assim como o andamento deste;
1.4. As informações sobre os chamados deverão permanecer armazenadas até o final do contrato, sendo possível acessá-las através do portal de atendimento por qualquer usuário da CONTRATANTE na solução;
1.5. A CONTRATADA deverá cumprir prazos máximos para resposta aos acionamentos (Tabela 1), de acordo com o nível de severidade de cada chamado:
1.5.1. Severidade ALTA: Esse nível de severidade é aplicado quando a solução se encontra totalmente indisponível ou funcionando de forma intermitente ou grande degradação de performance. Há uma falha nos componentes da solução que deixem indisponíveis seus recursos. Há impacto a todos os usuários.
1.5.2. Severidade MÉDIA: Esse nível de severidade é aplicado quando há falha, simultânea ou não, do uso da solução, em que se encontra parcialmente indisponível ou com degradação de performance ou perda de funcionalidades e serviços que afetem grande parte dos usuários;
1.5.3. Severidade BAIXA: Esse nível de severidade é aplicado quando a solução se encontra disponível, mas há ocorrência de alarmes, ou com pouco impacto a um ou mais usuários. Também quando for necessário realizar consulta sobre problemas ou dúvidas gerais sobre a solução, manutenções preventivas e corretivas não urgentes, atualizações de softwares, firmwares, reconfiguração de ambiente, ou ajustes não urgentes e necessários na solução para seu perfeito funcionamento
1.5.4. Severidade CONSULTORIA: Todas as atividades de consultoria.

Modalidade de atendimento	**Evento**	**Prazos para os níveis de severidade**			
		1 - ALTA	**2 - MÉDIA**	**3 - BAIXA**	**4 – CONSULTORIA**
On-Site, E-mail, ou Telefone	Término de atendimento	6 (seis) horas corridas	8 (doze) horas corridas	Até o 2º dia útil após a abertura do chamado	Até o 5º dia útil após a abertura do chamado

Tabela 1 – Tabela de prazos de atendimento.

1.6. Serão considerados para efeitos dos níveis exigidos:
1.6.1. Prazo de término de atendimento: tempo decorrido entre a abertura do chamado efetuada pela equipe técnica da CGU à CONTRTADA ou à fabricante e o retorno de disponibilidade da solução;
1.6.2. O nível de severidade será informado pela CONTRATANTE no momento da abertura de cada chamado;
1.6.3. O nível de severidade de um acionamento poderá ser reclassificado no decorrer do atendimento e conforme a disponibilidade de recursos dos módulos e componentes da solução;
1.6.4. Para os chamados de nível BAIXO e de CONSULTORIA, considera-se o horário comercial das 8:00h às 18:00h, sendo que se o chamado for aberto a partir das 15:00h, considera-se a contagem a partir das 08:00h do dia seguinte.
1.6.5. Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA, para acompanhamento e controle da execução do serviço;
1.6.6. A CONTRATADA apresentará à CONTRATANTE, ao término de cada atendimento, um relatório de atendimento técnico contendo dados sobre a intervenção na solução;
1.6.7. Caso a solução seja considerada insatisfatória, a CONTRATATANTE poderá efetuar a reabertura do chamado, onde continuará a contagem do tempo de atendimento.
1.6.8. A CONTRATADA também fornecerá atendimento técnico por meio de visitas presenciais à CONTRATANTE, para eventuais demandas que, uma vez esgotadas as tentativas de solução por meio de contato telefônico ou correio eletrônico, ainda não tenham sido solucionadas. Sempre que demandada neste sentido, a CONTRATADA alocará recursos para atendimento in loco, mediante prévio agendamento, para possibilitar a estruturação da visita já com a solução esquematizada. O relatório de visita deverá ser assinado pelo servidor da CONTRATANTE que solicitou o atendimento técnico;
1.6.9. O descumprimento dos prazos de atendimento da Tabela 1 implicará na aplicação de multas compensatória, conforme Tabela 2, assegurados o contraditório e a ampla defesa;
1.6.10. Nos casos em que atrasos na solução dos chamados técnicos se deem pela ocorrência de “bug”, notadamente reconhecido pelo fabricante do produto, a CONTRATADA poderá apresentar à CONTRATANTE exposição de motivos que fundamentem a ocorrência desta situação;

1.6.11. Caso a CONTRATANTE considere procedentes as justificativas apresentadas, poderá descontar do tempo total do chamado o tempo decorrido entre a identificação e a solução final para o "bug".
1.6.12. Caso seja a primeira ocorrência, ou nos casos de atraso inferior a 50% dos limites de atendimento estabelecidos, a CONTRATANTE poderá optar pela aplicação de advertência.
1.6.13. No caso de descumprimento dos prazos de atendimento estabelecidos, a Administração poderá aplicar as penalidades conforme a tabela abaixo.

Resultado esperados e níveis de qualidade exigidos	**Unidade de cálculo**	**Fórmula de cálculo da multa**	**Limite da multa**
ALTA	1 hora corrida	NHAT * 0,5% * VRS	5% do VRS
MÉDIA	1 hora corrida	NHAT * 0,5% * VRS	4% do VRS
BAIXA	1 dia útil	NDAT * 0,5% * VRS	3% do VRS
CONSULTORIA	1 dia útil	NDAT * 0,5% * VRS	2% do VRS

Tabela 2 – Aplicação de multas do serviço de suporte técnico de hardware e software

1.6.14. Onde:
1.6.14.1. VRS – Valor de Referência para Sanção = valor do bem contratado para o qual está sendo aberto o chamado;
1.6.14.2. NHAT – número de horas decorridas entre o final do prazo de atendimento e o efetivo término do atendimento;
1.6.14.3. NDAT – número de dias úteis decorridos entre o final do prazo de atendimento e o efetivo término do atendimento.
1.6.15. Deverá ser disponibilizado no portal de atendimento área de consulta do chamado, incluindo hora de abertura e fechamento assim como o andamento deste.
1.6.16. As informações sobre os chamados deverão permanecer armazenadas até o final do contrato, sendo possível acessá-las através do portal de atendimento por qualquer usuário da solução
1.6.17. Este documento possui período de vigência concomitante à vigência do contrato.

ANEXO III – MODELO DE TERMO DE COMPROMISSO CO NFIDENCIALIDADE

CONTRATO Nº _____ /20

A **<PESSOA JURÍDICA OU FÍSICA CONTRATADA>** doravante referida simplesmente como **CONTRATADA**, inscrita no CNPJ/MF sob o número <NÚMERO DO CNPJ>, com endereço <ENDEREÇO>, neste ato representada pelo <VÍNCULO DO SIGNÁRIO COM A CONTRATADA>, **<NOME DO SIGNATÁRIO>**, nos termos do <CONTRATO OU TERMO ADITIVO EM QUE FOI

PACTUADO O SIGILO>, compromete-se a observar o presente TERMO DE COMPROMISSO CONFIDENCIALIDADE, firmado perante a **UNIÃO**, por meio do **CONTROLADORIA-GERAL DA UNIÃO,** doravante referido simplesmente como **CGU**, em conformidade com as cláusulas que seguem:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste TERMO DE COMPROMISSO CONFIDENCIALIDADE é a necessária e adequada proteção às informações controladas de propriedade exclusiva da CGU fornecidas à CONTRATADA para que possa desenvolver as atividades contempladas especificamente no Contrato nº _____/_____.

Subcláusula Primeira - A CONTRATADA reconhece que, em razão da prestação de serviços à CGU, tem acesso a informações que pertencem à CGU, que devem ser tratadas como controladas.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

O termo “informações controladas de propriedade exclusiva da CGU” abrange toda informação, por qualquer modo apresentada ou observada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outras a que, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, venha a CONTRATADA ter acesso durante ou em razão da execução do contrato celebrado.

Subcláusula Primeira - Em caso de dúvida acerca da natureza confidencial de determinada informação, a CONTRATADA deverá mantê-la sob sigilo até que seja autorizada expressamente pelo representante legal da CGU, referido no Contrato, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa da CGU poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES

A CONTRATADA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa da CGU, das informações controladas reveladas.

Subcláusula Primeira – As informações de caráter técnico observadas ou informadas durante a execução do contrato que impactem especificamente os produtos ou serviços fornecidos e prestados pela CONTRATADA poderão ser utilizadas por essa para a melhoria de seus produtos, reparos ou mesmo compartilhados com outros clientes sem a necessidade de autorização prévia da CGU. Em nenhum momento o nome da CGU ou outra fonte poderá ser vinculada ou distribuída conjuntamente com a informação dos produtos da CONTRATADA.

Subcláusula Segunda - A CONTRATADA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços à CGU, as informações controladas reveladas.

Subcláusula Terceira - A CONTRATADA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços à CGU, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações controladas reveladas.

Subcláusula Quarta - A CONTRATADA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

Subcláusula Quinta - A CONTRATADA obriga-se a informar imediatamente à CGU qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

CLÁUSULA QUARTA - DO DESCUMPRIMENTO

A quebra do sigilo das informações controladas reveladas, devidamente comprovada, sem autorização expressa da CGU, possibilitará a imediata rescisão de qualquer contrato firmado entre a CGU e a CONTRATADA sem qualquer ônus para a CGU. Nesse caso, a CONTRATADA estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CGU, inclusive os de ordem moral, bem como as responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

CLÁUSULA QUINTA - DO RETORNO DAS INFORMAÇÕES

A CONTRATADA devolverá imediatamente à CGU, ao término do Contrato, todo e qualquer material de propriedade desta, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial, nos termos do presente TERMO DE COMPROMISSO CONFIDENCIALIDADE, a que teve acesso em decorrência do vínculo contratual com a CGU.

CLÁUSULA SEXTA - DA VIGÊNCIA

O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor a partir de sua assinatura e enquanto perdurar a natureza sigilosa ou restrita da informação, inclusive após a cessação da razão que ensejou o acesso à informação.

CLÁUSULA SÉTIMA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE COMPROMISSO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pela CGU.

Por estarem de acordo, a CONTRATADA, por meio de seu representante, firma o presente TERMO DE COMPROMISSO CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

Brasília, DF, _____ de _____ de _____.

<REPRESENTANTE DA CONTRATADA> <VÍNCULO DO REPRESENTANTE COM A CONTRATADA> RG: CPF:

DE ACORDO: (integrantes da equipe técnica da CONTRATADA) _____ _____	
Nome:	Nome:
RG:	RG:

ANEXO IV – MODELO DE TERMO DE CIÊNCIA

TERMO DE CIÊNCIA

INTRODUÇÃO
Visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos no projeto sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

IDENTIFICAÇÃO			
Contrato N°:			
Objeto:			
Contratante:	Controladoria-Geral da União		
Gestor do Contrato:		Matr.:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes na Contratante:

1. Portaria CGU nº 587/2021: Institui a Política de Segurança da Informação da Controladoria-Geral da União;
2. Norma Complementar nº 05/2017: Estabelece as diretrizes para o uso dos recursos de Tecnologia da Informação e Comunicação no âmbito da CGU; e
3. Código de Conduta da CGU;

CIÊNCIA	
CONTRATADA – Empregados	
_____ *<Nome>* **Matrícula: <*Matr.*>**	_____ *<Nome>* **Matrícula: <*Matr.*>**

_____,_____ de _____ de 20_____.

ANEXO V – MODELOS DE ORDEM DE SERVIÇO E DE ADITIVO

	CONTROLADORIA GERAL DA UNIÃO - CGU	**Nº da OS**
	Ordem de Serviço – Contrato nº __ / _____ Objeto: Serviços de link internet	**_____**
Tipo de OS		( ) Projeto ( )Manutenção
Nome do Projeto/Sistema(s)		
Data de Abertura		
Data Prevista de Término		
Quantitativo de links:		
		_____ Nome - Matrícula

Representantes da CGU:	(Representante da área de negócio - demandante) _____ Nome - Matrícula (Gestor ou Fiscal do Contrato)
Ciência do representante da empresa:	_____ Nome – Cargo na empresa

	CORREGEDORIA GERAL DA UNIÃO - CGU	
	Aditivo nº ____ à Ordem de Serviço – Contrato nº __ / _____ Objeto: Serviços link internet	**Nº da OS** **_____**

Tipo de OS:	( ) Projeto ( )Manutenção
Data do Aditivo:	
Tipo:	( ) Aumento de __ do link ( ) Redução de __ do link ( ) Prorrogação do Término da OS para __ / __ / ____ ( ) Antecipação do Término da OS para __ / __ / ____
	_____

Representantes da CGU	Nome - Matrícula (Representante da área de negócio - demandante) _____ Nome - Matrícula (Gestor ou Fiscal do Contrato)
Ciência do representante da empresa:	_____ Nome – Cargo na empresa

Obs: Estes modelos poderão ser alterados ou eventualmente substituídos por sistema informatizado visando melhor adequação à execução contratual.

2. 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 GUEDES PAYSAN

integrante Requisitante

Assinou eletronicamente em 22/12/2023 às 19:56:07.

PIERRY ANGELO PEREIRA

Integrante Técnico

Assinou eletronicamente em 26/12/2023 às 10:06:39.

ANDRESSA CRISTINA SANTOS DE DEUS

Integrante Administrativo

Assinou eletronicamente em 22/12/2023 às 17:34:02.

Despacho: De acordo. Encaminhe-se à Diretoria de Gestão Corporativa, para o obséquio das providências cabíveis em seu âmbito de atribuições.

HENRIQUE APARECIDO DA ROCHA

Autoridade Máxima de TIC

Assinou eletronicamente em 22/12/2023 às 17:52:48.