

COORDENAÇÃO-GERAL DE RECURSOS LOGÍSTICOS

Termo de Referência 177/2025

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
177/2025	390004-COORDENAÇÃO-GERAL DE RECURSOS LOGÍSTICOS	HENRIQUE ALCANTARA VELOSO MOTA	24/11/2025 16:44 (v 0.7)
Status	ASSINADO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Bens de TIC	45/2025	50000.026167/2024-54

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Registro de Preços para a eventual contratação de empresa especializada no fornecimento de Solução de Proteção de Rede Perimetral - Período de 60 meses, da empresa Fabricante Fortinet, incluída a Subscrição de todas as Licenças do Conjunto de Funcionalidades, serviços de implantação e transferência de tecnologia, garantia de atualização contínua do sistema operacional e suporte técnico de instalação durante o período de garantia, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

GRUPO	ITEM	ESPECIFICAÇÃO	CÓDIGO SIASG	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	1	Solução de Proteção de Rede Perimetral – Período de 60 meses	481646	Unidade	10	R\$ 1.445.000,00	R\$ 14.450.000,00
	2	Sistema de Gerência Centralizada – Período de 60 meses	27502	Unidade	5	R\$ 357.195,00	R\$ 1.785.975,00
	3	Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede	27502	Unidade	200	R\$ 2.109,65	R\$ 421.930,00
	4	Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede	27502	Unidade	4050	R\$ 284,12	R\$ 1.150.686,00

1.2. Estimativas de consumo individualizadas, do órgão gerenciador e órgãos(s) e entidade(s) participantes, bem como endereços de entregas:

Órgão Gerenciador: MINISTÉRIO DOS TRANSPORTES					
Item	Descrição/especificação	Unidade de medida	Requisição mínima	Requisição Máxima	Quantidade total
1	Solução de Proteção de Rede Perimetral – Período de 60 meses	Unidade	=	02	02
2	Sistema de Gerência Centralizada – Período de 60 meses	Unidade	=	01	01
3	Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede	Unidade	=	100	100
4	Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede	Unidade	=	1500	1500
ENDEREÇO DE ENTREGA: Esplanada dos Ministérios, Bloco R, Zona Cívico-Administrativa, Brasília, DF					

Órgão Participante: SECRETARIA DO CONSELHO DA JUSTICA FEDERAL-CFJ

Item	Descrição/especificação	Unidade de medida	Requisição mínima	Requisição Máxima	Quantidade total
1	Solução de Proteção de Rede Perimetral – Período de 60 meses	Unidade	=	04	04
2	Sistema de Gerência Centralizada – Período de 60 meses	Unidade	=	02	02
3	Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede	Unidade	=	0	0
4	Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede	Unidade	=	0	0
ENDEREÇO DE ENTREGA: SCES, LOTE 09, TRECHO 03, POLO 08, BRASÍLIA/DF					

Órgão Participante: TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ

Item	Descrição/especificação	Unidade de medida	Requisição mínima	Requisição Máxima	Quantidade total
1	Solução de Proteção de Rede Perimetral – Período de 60 meses	Unidade	=	02	02
2	Sistema de Gerência Centralizada – Período de 60 meses	Unidade	=	01	01
3	Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede	Unidade	=	100	100
4	Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede	Unidade	=	1500	1500
ENDEREÇO DE ENTREGA: AVENIDA ALMIRANTE BARROSO, BELÉM/PA					

Órgão Participante: INFRA S.A

Item	Descrição/especificação	Unidade de medida	Requisição mínima	Requisição Máxima	Quantidade total
1	Solução de Proteção de Rede Perimetral – Período de 60 meses	Unidade	=	02	02
2	Sistema de Gerência Centralizada – Período de 60 meses	Unidade	=	01	01
3	Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede	Unidade	=	0	0
04	Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede	Unidade	=	1050	1050
ENDEREÇO DE ENTREGA: SAUS QUADRA 1, BLOCO 'G', LOTES 3 E 5, BRASÍLIA/DF					

Classificação do objeto quanto à heterogeneidade ou complexidade

1.3. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar, uma vez que possuem padrões de desempenho, qualidade e características gerais que podem ser definidos de forma objetiva, por intermédio de especificações técnicas usualmente encontradas no mercado, podendo, portanto, ser licitado na modalidade jurídica do Pregão Eletrônico, nos termos do art. 6, inciso XIII da Lei nº 14.133/2021.

Classificação do objeto como bem de luxo

1.4. O objeto desta contratação não se enquadra como bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

Classificação do objeto quanto ao modelo de execução

1.5. O fornecimento de bens é enquadrado como continuado tendo em vista que é uma necessidade permanente, imprescindível para a manutenção das atividades deste Ministério, sendo a vigência plurianual mais vantajosa considerando o Estudo Técnico Preliminar.

Prazo de vigência

1.6. O prazo de vigência da contratação é de 5 (cinco) anos, contados da sua assinatura, prorrogável por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

1.7. O contrato ou outro instrumento hábil que o substitua oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

1.8. Em caso de divergência entre disposições deste Termo de Referência e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Termo de Referência.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A presente contratação justifica-se pela promoção de uma maior proteção de acessos aos ativos e sistemas deste Ministério, com o intuito de garantir a confidencialidade, integridade e disponibilidade dos dados transmitidos ou armazenados na infraestrutura de rede. A relação da necessidade e volumes necessários estão evidenciados nos itens nº 6 e 7 do Estudo Técnico Preliminar.

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

- I) ID PCA no PNCP: 37115342000167-0-000002/2025
- II) Data de publicação no PNCP: 21/03/2025
- III) Id do item no PCA: 156
- IV) Classe/Grupo: EQUIPAMENTOS DE REDE DE TIC - LOCAL E REMOTA
- V) Identificador da Futura Contratação: 390004-45/2025

2.3. O objeto da contratação também está alinhado com a Estratégia Nacional de Governo Digital - ENGD (2024-2027), com o Planejamento Estratégico Institucional - PEI (2024-2027) e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC (2024-2026) do Ministério dos Transportes, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
OBJETIVO	OBJETIVOS ESTRATÉGICOS ENGD 2024-2027
6	Recomendação 6.2. Adotar e contribuir para formação de arranjos colaborativos de disponibilização de infraestrutura e soluções digitais, fomentando inclusive a participação das empresas públicas de tecnologia de informação nesses arranjos.
6	Recomendação 6.4. Estabelecer iniciativas para prover e qualificar o acesso a infraestruturas de rede, especialmente as de grande tráfego, para maior eficiência de trabalho em prédios e equipamentos públicos, considerando inclusive parcerias e programas nacionais voltados para essa finalidade.
EIXO	OBJETIVOS ESTRATÉGICOS PEI 2024-2027
DADOS	7: Implementar estratégias de dados para posicionar o Ministério dos Transportes como indutor de soluções que otimizem a comunicação com a sociedade e a produtividade do Brasil.
DESENVOLVIMENTO INSTITUCIONAL	6: Desenvolver capacidade institucional do Ministério dos Transportes com foco em excelência e produtividade para atendimento dos desafios prioritários.
GOVERNANÇA CORPORATIVA	8: Fortalecer a governança colaborativa com governo e sociedade para garantir a efetividade das políticas públicas.

ALINHAMENTO AO PDTIC 2024-2026			
AC	AÇÕES (AC)	OTI	OBJETIVO ESTRATÉGICO DE TI (OTI)
4.3.1.1	Atualização da infraestrutura de Tecnologia da Informação e Comunicação.	OTI4	Atualizar Parque Tecnológico
6.1.1.3	Desenvolver e Implementar a Política de Controle de Acesso	OTI6	Promover a Segurança da Informação
6.1.1.4	Desenvolver e Implementar a Política de Gestão de Registro (Logs) de Auditoria	OTI6	Promover a Segurança da Informação

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

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3.2. A solução de TIC consiste no fornecimento de Solução de Proteção de Rede Perimetral conforme especificação técnica pormenorizada no Anexo A - Caderno de Especificação Técnica deste Termo de Referência.

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio

4.1. Os Requisitos de Negócios descritos para esta contratação encontram-se pormenorizados no Tópico 4 - Necessidades de Negócios, subitem 4.6 do Estudo Técnico Preliminar - ETP.

Requisitos de Capacitação

4.2. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação.

Requisitos Legais

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

4.3.1 A contratada deverá se submeter à Política de Segurança da Informação (POSIN) do Ministério dos Transportes, nos termos da Portaria n.º 287, de 4 de abril de 2025.

4.3.2 Decreto nº 11.246, de 27 de outubro de 2022 - Regulamenta o disposto no § 3º do art. 8º da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre as regras para a atuação do agente de contratação e da equipe de apoio, o funcionamento da comissão de contratação e a atuação dos gestores e fiscais de contratos, no âmbito da administração pública federal direta, autárquica e fundacional.

4.3.3 Lei nº 8.248, de 23 de outubro de 1991 - Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.

4.3.4 Decreto nº 7.174, de 12 de maio de 2010 – Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.

4.3.5 Decreto nº 11.462, de 31 de março de 2023 - Regulamenta os art. 82 a art. 86 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional.

4.3.6 Lei Complementar nº 123, de 14 de dezembro de 2006 - Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte.

4.3.7 Decreto nº 8.538, de 6 de outubro de 2015 - Regulamenta o tratamento favorecido, diferenciado e simplificado para microempresas, empresas de pequeno porte, agricultores familiares, produtores rurais pessoa física, microempreendedores individuais e sociedades cooperativas nas contratações públicas de bens, serviços e obras no âmbito da administração pública federal.

4.3.8 Instrução Normativa SLTI/MPOG nº 1, de 19 de janeiro de 2010 - Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.

4.3.9 Instrução Normativa SEGES/ME nº 77, de 4 de novembro de 2022 - Dispõe sobre a observância da ordem cronológica de pagamento das obrigações relativas ao fornecimento de bens, locações, prestação de serviços e realização de obras, no âmbito da Administração Pública federal direta, autárquica e fundacional.

4.3.10 Instrução Normativa SEGES/ME nº 53, de 8 dezembro de 2020 - Dispõe sobre as regras e os procedimentos para operação de crédito garantida por cessão fiduciária dos direitos de créditos decorrentes de contratos administrativos, realizadas entre o fornecedor e instituição financeira, por meio do Portal de Crédito digital, no âmbito da Administração Pública federal direta, autárquica e fundacional.

Requisitos de Manutenção

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

4.5. Será exigido garantia evolutiva de, no mínimo, **60** (sessenta) meses, podendo ser prorrogado até o limite decenal, devendo o acesso para downloads de patches, drivers e quaisquer outras atualizações necessárias estar disponível 24x7 (vinte e quatro horas por dia, sete dias por semana), durante todo o período de vigência do programa de licenciamento, podendo ser feito por meio de http ou ftp no sítio do fabricante do appliance.

4.6. A Contratada deve garantir ao Contratante o direito de atualizar o appliance para as novas versões disponibilizadas, durante todo o período de vigência do programa e sempre que julgar necessário. As novas versões devem estar disponíveis para download no sítio do fabricante do appliance.

4.7. Atualizações de segurança e correções de problema das versões instaladas (vícios do produto) deverão ser disponibilizadas durante todo o prazo de validade técnica da versão utilizada pelo Ministério dos Transportes, independente de possuir programa de licenciamento vigente, conforme Lei 8.078 /1990, art. 26, § 3º, e art. 39, inciso I e II, c/c Lei 9.609/1998, arts. 7º e 8º.

Requisitos Temporais

4.8. A Entrega dos equipamentos deverá ser efetivada no prazo máximo de **45** (quarenta e cinco) dias corridos, a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante.

4.9. A Ordem de Fornecimento de Bem - OFB indicará a quantidade, os endereços de entrega e da instalação e nome do responsável pelo recebimento, acompanhado de e-mail e/ou telefone para contato, além da solicitação de entrega do Projeto Provisório de Instalação - PPI.

4.10. A Contratada deverá informar à Contratante, quando da entrega dos equipamentos com, no mínimo, **5** (cinco) dias corridos de antecedência, ficando a Contratada responsável pelo transporte e entrega dos equipamentos e partes componentes da solução integrada de segurança da informação.

4.11. A Contratada será responsável por elaborar e entregar o Projeto Provisório de Instalação - PPI dos equipamentos em até **10** (dez) dias corridos, contados a partir da solicitação da Contratante.

4.12. A Contratante fará análise e validação do Projeto Provisório de Instalação – PPI, em até **3** (três) dias úteis, apontando as devidas correções e ou ajustes no documento, ficando a Contratada responsável por ajustar o plano em até **2** (dois) dias úteis, a partir da comunicação da Contratante das não conformidades e das alterações necessárias, apontadas pela Contratante.

4.13. A substituição do equipamento que apresentar divergência na especificação técnica, falhas de componentes, defeitos de fabricação e operação ou qualquer outro defeito apresentado durante o transporte, a entrega e a instalação dos equipamentos deverão ser efetuadas em até **5** (cinco) dias úteis, contados a partir da notificação da ocorrência por parte da Contratante.

4.14. A Contratada deverá entregar o Projeto Definitivo de Instalação - PDI (“As Built”) em até **2** (dois) dias úteis após a instalação.

4.15. Após a Contratada concluir toda a instalação dos equipamentos, deixando-os completamente operacionais, e a entrega de toda documentação técnica e do Projeto Definitivo de Instalação - PDI, conforme condições e prazos exigidos no Estudo Técnico Preliminar - ETP, a Contratante emitirá o Termo de Recebimento Provisório, em até **5** (cinco) dias úteis, contados a partir da comunicação de conclusão da instalação.

4.16. Após **15** (quinze) dias úteis da emissão do Termo de Recebimento Provisório, sendo confirmada a operação e desempenho a contento dos equipamentos, nos termos das especificações técnicas e do atestado de homologação, a Contratante emitirá o Termo de Recebimento Definitivo.

Atividade, Tarefa ou Serviço	Prazo
Ordem de Fornecimento de Bens	D
Entrega dos Bens	D + 45 (corridos)
Entrega do PPI	D + 10 (corridos)
Análise do PPI	D + 10 (corridos) + 3(úteis)
Ajuste do PPI	D + 10 (corridos) + 5 (úteis)
Instalação dos Equipamentos	D + 40 (corridos) + 10 (úteis)
Substituição de equipamentos na entrega	D + 40 (corridos) + 15 (úteis)
Projeto Definitivo de Instalação	D + 40 (corridos) + 17 (úteis)
Início do Treinamento	D + 30 (corridos)

4.17. Prazo para resolução de problemas técnicos será de:

- I** - Substituição de equipamento e/ou módulo que apresente pane/falha ou não conformidade técnica que o torne total ou parcialmente inoperante: **24** (vinte e quatro) horas, podendo ser prorrogado por igual período mediante justificativa autorizada pela Contratante;
- II** - Problema com impacto que cause restrições de operação de funções essenciais que torne o equipamento totalmente inoperante: **4** (quatro) horas;
- III** - Problema com impacto que cause restrições de operação de funções essenciais que torne o equipamento parcialmente inoperante: **6** horas;
- IV** - Problema sem impacto em operação que apresente pane/falha ou não conformidade técnica que causa restrições de operação de funções acessórias: **24** (vinte e quatro) horas;
- V** - Consulta: necessidade de resolver dúvidas sobre configuração, customização, otimização, operacionalização, uso e administração dos equipamentos e/ou módulos: **24** (vinte e quatro) horas;
- VI** - Disponibilizar atualização das versões de “firmware” para os equipamentos: **24** (vinte e quatro) horas.

Problemas Técnicos	Prazo para resolução
Substituição de equipamento e/ou módulo que apresente pane/falha ou não conformidade técnica que o torne total ou parcialmente inoperante	48h
Problema com impacto que cause restrições de operação de funções essenciais que torne o equipamento totalmente inoperante	4h
Problema com impacto que cause restrições de operação de funções essenciais que torne o equipamento parcialmente inoperante	6h
Problema sem impacto em operação que apresente pane/falha ou não conformidade técnica que causa restrições de operação de funções acessórias	24h
Consulta: necessidade de resolver dúvidas sobre configuração, customização, otimização, operacionalização, uso e administração dos equipamentos e/ou módulos	24h
Disponibilizar atualização das versões de “firmware” para os equipamentos	24h

4.18. Demais prazos pertinentes a prestação dos serviços de Suporte Técnico serão definidos oportunamente na forma de Níveis Mínimos de Serviços - NMS.

Requisitos de Segurança e Privacidade

4.19. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante.

Requisitos Sociais, Ambientais e Culturais

4.20. Os equipamentos devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

4.20.1 Os equipamentos devem estar aderentes às diretrizes sociais, ambientais e culturais constantes na Lei nº 12.305, de 2 de agosto de 2010, que Institui a Política Nacional de Resíduos Sólidos, além dos normativos relativos à sustentabilidade ambiental aplicáveis.

Requisitos da Arquitetura Tecnológica

4.21. Os equipamentos deverão atender integralmente aos requisitos de arquitetura tecnológica, conforme especificação técnica pormenorizada no Anexo A - Caderno de Especificação Técnica.

Requisitos de Projeto e de Implementação

4.22. Os equipamentos deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir:

4.22.1 A implantação deve ser por meio de projeto com cronograma, atividades e estrutura.

4.22.2 Após a emissão da Ordem de Fornecimento de Bens, a Contratada deverá apresentar Projeto Provisório de Implantação - PPI dos equipamentos, que será analisado e aprovado pela Contratante.

4.22.3 Após a instalação dos equipamentos e a aprovação da Contratante, a Contratada deverá apresentar o Projeto Definitivo de Implantação - PDI dos equipamentos.

Requisitos de Implantação

4.23. Os serviços deverão observar integralmente os requisitos de implantação, instalação e fornecimento especificados no Anexo A - Caderno de Especificação Técnica.

Requisitos de Garantia, Manutenção e Assistência Técnica

4.24. O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, **60** (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do Termo de Recebimento Definitivo do objeto.

4.25. Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.

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

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

4.28. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

4.29. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

4.30. Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até **24** (vinte e quatro) horas, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

4.31. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

4.32. Na hipótese do subitem acima, o Contratado deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

4.33. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

4.34. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.

4.35. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

4.36. Todos os custos decorrentes da retirada de equipamentos ou componentes para a prestação do serviço de garantia serão de responsabilidade da Contratada, bem como seu retorno aos locais onde serão instalados os equipamentos pela Contratada.

4.37. Os serviços de suporte técnico deverão ser prestados sempre que solicitados, em regime 24x7x365, por meio da abertura de Chamado Técnico via Central de Atendimento:

4.37.1 A Contratada deverá disponibilizar à Contratante uma Central de Atendimento de Chamados em língua portuguesa (telefone, sistema WEB e e-mail), constituída de estrutura de pronto atendimento em regime 24x7x365, para abertura de chamados e consultas com técnico especializado na solução em uso pela Contratante, com conhecimento para solucionar problemas e esclarecer dúvidas, de forma rápida e eficiente.

4.37.2 Deve ser possível o acionamento para solução de problemas decorrentes de defeitos e falhas nos equipamentos/software, ou seja, problemas decorrentes do fato do ativo de rede não realizar uma funcionalidade especificada ou esperada.

4.37.3 Poderá ainda, esse serviço, ser usado para solicitar informações quanto às dúvidas, funcionalidades e quanto a procedimentos para configuração dos itens da solução contratada.

4.37.4 Os serviços de suporte técnico serão prestados, preferencialmente, de forma remota, excetuando-se os casos em que não seja possível acessar a rede de dados da Contratante ou seja solicitada uma ação e intervenção On-Site (no local onde está o equipamento), para a execução completa das tarefas.

4.37.5 Em qualquer caso, a Contratada deverá arcar com todos os procedimentos necessários à solução do problema, incluindo a substituição de quaisquer módulos defeituosos no(s) equipamento(s), bem como a substituição do(s) próprio(s) equipamentos(s), se for necessário.

4.37.6 Um chamado somente poderá ser fechado após confirmação do Gestor/Fiscais do Contrato e apresentação de Relatório de Suporte pela Contratada, sendo que o término de atendimento se dará com a disponibilidade do recurso em perfeitas condições de operação e de uso.

4.38. Em caso de problema de software, os seguintes prazos máximos deverão ser obedecidos para o início do atendimento e término da correção do problema:

4.38.1 Problemas de alto impacto (indisponibilidade total): **2** (duas) horas para o início do atendimento e **4** (quatro) horas para o término da correção do problema, contados a partir da solicitação.

4.38.2 Problemas de médio impacto (lentidão ou indisponibilidade parcial): **6** (seis) horas para o início do atendimento e **24** (vinte e quatro) horas para o término da correção do problema, contados a partir da solicitação.

4.38.3 Problemas de baixo impacto (que não causem lentidão ou indisponibilidade): **6** (seis) horas para o início do atendimento e **10** (dez) dias para o término da correção do problema, contados a partir da solicitação.

Atividades	Prazo
Problemas de alto impacto (indisponibilidade total)	2 (duas) horas para o início do atendimento e 4 (quatro) horas para o término da correção do problema, contados a partir da solicitação
Problemas de médio impacto (lentidão ou indisponibilidade parcial)	6 (seis) horas para o início do atendimento e 24 (vinte e quatro) horas para o término da correção do problema, contados a partir da solicitação
Problemas de baixo impacto (que não causem lentidão ou indisponibilidade)	6 (seis) horas para o início do atendimento e 10 (dez) dias para o término da correção do problema, contados a partir da solicitação

4.39. Caso algum componente da solução entre em modo End-Of-Sale, End-Of-Support ou End-Of-Life, deverá ser substituído por outro com características iguais ou superiores conforme validação da Equipe Técnica para manter a continuidade do negócio.

Requisitos de Experiência Profissional

4.40. Os serviços de assistência técnica e garantia deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como, com todos os recursos ferramentais necessários para a prestação dos serviços.

Requisitos de Formação da Equipe

4.41. Não serão exigidos requisitos de formação da equipe para a presente contratação.

Requisitos de Metodologia de Trabalho

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

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

4.44. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento **24** horas por dia e **7** dias por semana de maneira eletrônica e **10** horas por dia e **5** dias por semana por via telefônica.

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

Requisitos de Segurança da Informação e Privacidade

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

4.46.1 Os tratamentos das demandas de atendimento remoto, assistência técnica e garantia deverão ser registrados em sistema informatizado nos moldes descritos neste Termo, sendo assegurado o acesso aos técnicos designados pela CONTRATADA, respeitando as Políticas de Segurança da Informação e de Uso Aceitável dos Recursos Informatizados da CONTRATANTE.

4.46.2 Promover o afastamento em relação ao objeto da contratação, no prazo máximo de **24** (vinte e quatro) horas após o recebimento da notificação, de qualquer dos seus recursos técnicos e/ou humanos que não correspondam aos critérios de confiança ou que perturbe a ação da equipe de fiscalização da CONTRATANTE.

Sustentabilidade

4.47. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.47.1 Use produtos de limpeza e conservação de superfícies e objetos inanimados que obedeçam às classificações e especificações determinadas pela ANVISA.

4.47.2 No que couber, visando a atender o disposto na legislação aplicável, em destaque a IN SGD-ME nº 94/2022 e a IN SEGES-ME nº 98 /2022, 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.

4.47.3 Ainda como forma de atender aos requisitos constantes na seção específica de “Tecnologia da Informação e Comunicação - aquisição de (ou serviços que utilizem) bens de informática e automação” do Guia Nacional de Contratações Sustentáveis da Advocacia Geral da União (AGU. Guia Nacional de Contratações Sustentáveis da Advocacia Geral da União. Brasília: AGU, 2023, pp. 273-281, disponível em: <https://www.gov.br/agu/pt-br/composicao/cgu/cgu/guias/guia-de-contratacoes-sustentaveis-set-2023.pdf>, acesso 24/07/2023), os licitantes deverão atentar-se para as seguintes exigências:

4.47.3.1 Só será admitida a oferta de hardware que cumpra os critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos na Portaria nº 170, de 2012 do INMETRO.

4.47.3.2 Só será admitida a oferta de 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).

Indicação de marcas ou modelos:

4.48. Na presente contratação será admitida a indicação da(s) seguinte(s) marca(s), característica(s) ou modelo(s), de acordo com as justificativas contidas nos Estudos Técnicos Preliminares: itens 8 a 12.

Subcontratação

4.49. Não será admitida a subcontratação do objeto contratual.

Garantia da Contratação

4.50. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, podendo o Contratado optar pela caução em dinheiro ou em títulos da dívida pública, seguro-garantia, fiança bancária ou título de capitalização, em valor correspondente a **5%** (cinco por cento) do valor **total** da contratação.

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

4.51.1 A apólice de seguro-garantia permanecerá em vigor mesmo que o Contratado não pague o prêmio nas datas convencionadas.

4.51.2 Caso o adjudicatário não apresente a apólice de seguro de garantia antes da assinatura do contrato, ocorrerá a preclusão do direito de escolha dessa modalidade de garantia.

4.51.3 A apólice de seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

4.51.4 Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvados os períodos de suspensão contratual.

4.51.5 Caso o adjudicatário não opte pelo seguro-garantia ou não apresente a apólice de seguro de garantia antes da assinatura do contrato, deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contado da assinatura do contrato, comprovante de prestação de garantia nas modalidades de caução em dinheiro ou títulos da dívida pública, fiança bancária ou títulos de capitalização.

4.52. Caso seja a garantia em dinheiro a modalidade de garantia escolhida pelo Contratado, deverá ser efetuada em favor do Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

4.53. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério competente.

4.54. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

4.55. Na hipótese de opção pelo título de capitalização, a garantia deverá ser custeada por pagamento único, com resgate pelo valor total, sob a modalidade de instrumento de garantia, emitido por sociedades de capitalização regulamente constituídas e autorizadas pelo Governo Federal.

4.55.1 O título de capitalização deverá ser apresentado ao Contratante juntamente com as condições gerais e o número do processo administrativo sob o qual o plano de capitalização foi aprovado pela Susep (art. 8º, III, da Circular SUSEP nº 656, de 11 de março de 2022).

4.56. A garantia assegurará, qualquer que seja a modalidade escolhida, sob pena de não aceitação, o pagamento de:

4.56.1 prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas; e

4.56.2 multas moratórias e punitivas aplicadas pela Administração ao Contratado.

4.57. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, no prazo máximo de **10** (dez) dias úteis, prorrogáveis por igual período, contado da data de assinatura do termo aditivo ou da emissão do apostilamento, seguindo os mesmos parâmetros utilizados quando da contratação.

4.58. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o Contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

4.59. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contados da data em que for notificada.

4.60. O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

4.60.1 O emitente da garantia ofertada pelo Contratado deverá ser notificado pelo Contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

4.60.2 Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

4.61. Extinguir-se-á a garantia com a restituição da carta fiança, autorização para a liberação de importâncias depositadas em dinheiro a título de garantia ou anuência ao resgate do título de capitalização, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que o Contratado cumpriu todas as cláusulas do contrato.

4.61.1 A extinção da garantia na modalidade seguro-garantia observará a regulamentação da Susep.

4.61.2 A Administração deverá apurar se há alguma pendência contratual antes do término da vigência da apólice.

4.62. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

4.63. O Contratado autoriza o Contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

4.64. O garantidor não é parte para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções ao Contratado.

4.65. A garantia de execução é independente de eventual garantia do produto ou serviço prevista neste Termo de Referência.

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

4.66. A demanda do órgão tem como base as seguintes características:

4.66.1 A proposta da licitante deverá conter a especificação clara e completa do objeto, obedecida a mesma ordem constante deste Termo de Referência, sem conter alternativas de preços, ou de qualquer outra condição que induza o julgamento a ter mais de um resultado, conforme Modelo de PROPOSTA DE PREÇOS constante no ANEXO "B", deste TERMO DE REFERÊNCIA.

4.66.2 Entende-se por especificação clara e completa do objeto, o detalhamento do objeto, os quantitativos de serviços a serem entregues, marcas /modelos de aparelhos/equipamentos a serem fornecidos e demais condições gerais de prestação dos serviços que deverão constar da proposta da licitante.

4.66.3 Não serão aceitas propostas contendo cópia das exigências deste TERMO DE REFERÊNCIA no lugar da especificação clara e inequívoca dos serviços a serem contratados.

4.66.4 A licitante vencedora deverá apresentar planilha de preços, discriminando os valores total e unitário de cada item.

4.66.5 A proposta da licitante deverá estar integralmente preenchida, discriminando os valores unitários e totais de cada item objeto deste TERMO DE REFERÊNCIA, em conformidade com o modelo constante do ANEXO "B".

Justificativa de não aplicação da reserva de cotas

4.67. A não aplicação da reserva fundamenta-se no art. 6º, III, do Decreto nº 8.538/2015, que dispensa a cota quando o objeto for tecnológico e indivisível, e nos arts. 48 a 50 da Lei Complementar nº 123/2006, que a tornam obrigatória apenas quando tecnicamente possível. O firewall NGFW depende de licenciamento unificado, garantia do fabricante e suporte especializado, impossibilitando o fracionamento. O entendimento é reforçado pelas contratações similares e pelo Acórdão 3.236/2021-TCU, que classifica bens de TIC especializados como não passíveis de divisão. Assim, a reserva de cotas é inaplicável ao presente certame.

Análise sobre a possibilidade de aplicação da reserva de cotas para MEs/EPPs

4.68. A reserva de cotas não é aplicável ao objeto desta contratação, pois o item principal — firewall de próxima geração (NGFW) — é um bem de tecnologia avançada, de natureza complexa e indivisível, cuja divisão comprometeria a integridade da solução. Nas contratações similares analisadas no PNCP, a ampla maioria dos órgãos afastou a reserva justamente pela indivisibilidade técnica do equipamento, aplicando cotas apenas, quando muito, a serviços acessórios. Assim, não há viabilidade técnica para fracionamento competitivo.

Margem de Preferência

4.69. O objeto da contratação não se enquadra em qualquer margem de preferência, seja normal ou adicional, prevista em Decreto específico ou em Resoluções da Comissão Interministerial de Contratações Públicas para o Desenvolvimento Sustentável – CICS.

4.70. A CICS não possui Resolução vigente que atribua margens de preferência para equipamentos de segurança de redes, firewalls, appliances de TIC, softwares ou licenças, nem tampouco há bens manufaturados nacionais equivalentes que atendam às normas técnicas aplicáveis.

4.71. Dessa forma, não há margem de preferência aplicável, nos termos do art. 26 da Lei nº 14.133/2021 e do Decreto nº 11.317/2022.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

5.1.1 nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2 encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3 receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

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

5.1.5 liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6 comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7 definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável; e

5.1.8 prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.2. São obrigações do CONTRATADO

5.2.1 indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;

5.2.2 atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

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

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

5.2.5 manter, durante toda a execução do contrato, as mesmas condições da habilitação;

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

5.2.7 quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

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

5.2.9 fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso.

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

5.3.1 efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

5.3.2 conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

5.3.3 definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.3.3.1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

5.3.3.2. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

5.3.4 definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

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

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

5.3.4.3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 deste artigo, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6. MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de execução

Do Encaminhamento Formal de Demandas

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

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

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

Forma de execução e acompanhamento do contrato

Condições de Entrega

6.4. O prazo de entrega dos bens é de **45** (quarenta e cinco) dias corridos, contados do(a) emissão da Ordem de fornecimento de bens (OFB), em remessa única.

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

6.6. Os bens deverão ser entregues nos endereços nos quadros 1.2., além das orientações detalhadas na OFB.

Formas de transferência de conhecimento

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

6.7.1 Será necessário transferência de conhecimento à equipe que atuará com a solução. A transferência de conhecimento deverá ser de no mínimo 20 (vinte) horas de duração;

6.7.2 O conteúdo deverá abranger todas as funcionalidades e abordar as especificidades do projeto de implantação que sejam necessárias para manter as Soluções Funcionais;

6.7.3 Abranger todas as funcionalidades especificadas no Anexo "A"; e

6.7.4 Serem fornecidos certificados de participação para cada participante..

Procedimentos de transição e finalização do contrato

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

Quantidade mínima de serviços para comparação e controle

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

Mecanismos formais de comunicação

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

- I)** Ordem de Serviço;
- II)** Ata de Reunião;
- III)** Ofício;
- IV)** Sistema de abertura de chamados;
- V)** E-mails e Cartas;

Formas de Pagamento

6.11. Os critérios de medição e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato.

Manutenção de Sigilo e Normas de Segurança

6.12. 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.

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

7. MODELO DE GESTÃO DO CONTRATO

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

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

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

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

Reunião Inicial

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

7.6. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até **10** (dez) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.7. A pauta desta reunião observará, pelo menos:

- 7.7.1** Presença do representante legal da contratada, que apresentará o seu preposto;
- 7.7.2** Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;
- 7.7.3** esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

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

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

Fiscalização

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

Fiscalização Técnica

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

7.10. 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.

7.11. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.12. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.13. 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.

7.14. 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.

Fiscalização Administrativa

7.15. 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 da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.16. 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.

7.17. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da Contratante ou de seus agentes, gestores e fiscais, de conformidade.

Gestor do Contrato

7.18. Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

7.18.1 coordenar 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.

7.18.2 acompanhar 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.

7.18.3 acompanhar a manutenção das condições de habilitação da contratada, 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.

7.18.4 emitir 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.

7.18.5 tomar 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.

7.18.6 elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

7.18.7 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.

7.19. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual.

Critérios de Aceitação

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

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

7.22. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

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

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

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

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

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

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

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

Procedimentos de Teste e Inspeção

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

7.30.1 Previamente ao recebimento definitivo da solução serão realizados a verificação, testes e inspeção do atendimento integral às especificações técnicas exigidas. Estas ações serão realizadas por equipe designada.

7.30.2 Inicialmente deverá ser realizada a verificação das especificações exigidas através da inspeção física dos equipamentos.

7.30.3 Análise dos manuais técnicos enviados juntamente com os equipamentos ou disponibilizados de alguma forma e da análise de informações disponibilizadas no site da fabricante. Para esta etapa deve-se observar a seguinte lista de verificação:

7.30.3.1. Verificar se a caixa do equipamento foi entregue lacrada, em embalagem original e apresentando identificações de marca e modelo de acordo a descrição da proposta da CONTRATADA;

7.30.3.2. Verificar se o equipamento está novo e sem uso;

7.30.3.3. Verificar se o equipamento é o mesmo equipamento que foi ofertado na proposta;

- 7.30.3.4.** Verificar se o equipamento foi entregue acompanhado de todos os acessórios previstos nas especificações técnicas (como cabo de energia, conectores, etc.) e descritos na documentação apresentada junto com a proposta da CONTRATADA;
- 7.30.3.5.** Verificar se o(s) equipamentos(s) foram entregues na(s) quantidade(s) correta(s);
- 7.30.3.6.** Verificar se a documentação mínima exigida foi entregue (exceto relatório de implantação);
- 7.30.3.7.** Verificar se os equipamentos foram recebidos com a tensão elétrica adequada;

7.30.4. Após, deverá ser conduzida a inspeção através da verificação da conformidade da execução dos serviços em relação aos requisitos exigidos nas especificações técnicas. Para avaliação, serão considerados relatórios das ferramentas, verificação das configurações, testes de uso das funcionalidades, documentações de projeto, manuais das soluções e quaisquer outros documentos pertinentes.

Níveis Mínimos de Serviço Exigidos

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

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO		
Tópico	Descrição	
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens.	
Meta a cumprir	IAE < = 0	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento de Bens dentro do prazo previsto.
Instrumento de medição	OFB, Termo de Recebimento Provisório (TRP)	
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OFB. Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB.	
Periodicidade	Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.	
Mecanismo de Cálculo (métrica)	<p>IAE = <u>TEX – TEST</u></p> <p>Onde:</p> <p>IAE – Indicador de Atraso de Entrega da OFB;</p> <p>TEX – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB.</p> <p>A data de início será aquela constante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB.</p> <p>A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quanto o Contratado entrega os produtos da OFB e haja aceitação por parte do fiscal técnico.</p> <p>TEST – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.</p>	
Observações	Obs1: Serão utilizados dias corridos na medição.	

	Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.
Início de Vigência	A partir da emissão da OFB.
Faixas de ajuste no pagamento e Sanções	<p>Para valores do indicador IAE:</p> <p>Menor ou igual a 0 – Pagamento integral da OFB;</p> <p>De 1 a 60 - aplicar-se-á glosa de 0,1666% por dia de atraso sobre o valor da OFB ou fração em atraso.</p> <p>Acima de 60 - aplicar-se-á glosa de 10% bem como multa de 2% sobre o valor OFB ou fração em atraso.</p>

8. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NOS PAGAMENTOS

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

Id	Ocorrência	Glosa / Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução do contrato, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 01 (um) dia útil.	Multa de 0,5% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela contratante, até o limite de 10 (dez) dias.
		Após o limite de 10 (dez) dias úteis, aplicar-se-á multa de 10 (dez) % do valor total do Contrato.
2	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS)	De 1 a 10 (dias de atraso) – Glosa de 5% sobre o valor da OS.
		De 10 a 15 (dias de atraso) – Glosa de 10% sobre o valor da OS.
		De 15 a 30 (dias de atraso) - Glosa de 15% sobre o valor da OS.
3	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	<p>Advertência.</p> <p>Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 0,5 (zero vírgula cinco) % do valor total do Contrato.</p>

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

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

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

8.3. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) der causa à inexecução parcial do contrato;

- b)** der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c)** der causa à inexecução total do contrato;
- d)** ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e)** apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f)** praticar ato fraudulento na execução do contrato;
- g)** comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h)** praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

8.4. Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

8.4.1 Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

8.4.2 Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

8.4.3 Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

8.4.4 Multa:

8.4.4.1. Moratória, para as infrações descritas no item “d”, de **0,5%** (zero vírgula cinco por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de **10** (vinte) dias;

8.4.4.2. Moratória de **0,5%** (zero vírgula cinco por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia;

8.4.4.2.1 O atraso superior a 10 (dez) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

8.4.4.3. Compensatória, para as infrações descritas acima alíneas “e” a “h” de **0,5%** (zero vírgula cinco por cento) a **10%** (dez por cento) do valor da contratação.

8.4.4.4. Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de **5%** (cinco por cento) a **30%** (trinta por cento) do valor da contratação.

8.4.4.5. Compensatória, para a infração descrita acima na alínea “b”, de **0,5%** (zero vírgula cinco por cento) a **20%** (vinte por cento) do valor da contratação.

8.4.4.6. Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de **0,5%** (zero vírgula cinco por cento) a **10%** (dez por cento) do valor da contratação.

8.4.4.7. Compensatória, para a infração descrita acima na alínea “a”, de **1%** (um por cento) a **10%** (dez por cento) do valor da contratação, ressalvadas as seguintes infrações também enquadráveis nessa alínea:

8.4.4.7.1 Falha na entrega de relatórios técnicos mensais exigidos em contrato;

8.4.4.7.2 Não atualização tempestiva das bases de detecção e assinaturas;

8.4.4.7.3 Atraso na disponibilização do acesso ao sistema de gerenciamento centralizado;

8.4.4.7.4 Não apresentação do plano de implantação nos prazos definidos;

8.4.4.7.5 Falhas parciais na operação que não comprometam a disponibilidade total do serviço.

8.5. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

8.6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

8.7. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

8.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

8.9. A multa poderá ser recolhida administrativamente no prazo máximo de **15** (quinze) dias úteis, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

8.10.1 Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

8.10.2 Os endereços de e-mail informados na proposta comercial e/ou cadastrados no SICAF serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

8.11. Na aplicação das sanções serão considerados:

8.11.1 a natureza e a gravidade da infração cometida;

8.11.2 as peculiaridades do caso concreto;

8.11.3 as circunstâncias agravantes ou atenuantes;

8.11.4 os danos que dela provierem para o Contratante; e

8.11.5 a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

8.12. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

8.13. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

8.14. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

8.14.1 As penalidades serão obrigatoriamente registradas no SICAF.

8.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

8.16. Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do objeto

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

9.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de **15** (quinze) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

9.3. O recebimento definitivo ocorrerá no prazo de **5** (cinco) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

9.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até **10** (dez) dias úteis.

9.5. 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.

9.6. 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 quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

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

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

9.9. As atividades de montagem, instalação e quaisquer outras necessárias para o funcionamento ou uso do bem correrão por conta do Contratado e são condição para o recebimento do objeto.

Liquidação

9.10. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

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

9.12. 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:

9.12.1 o prazo de validade;

9.12.2 a data da emissão;

9.12.3 os dados do contrato e do órgão Contratante;

9.12.4 o período respectivo de execução do contrato;

9.12.5 o valor a pagar; e

9.12.6 eventual destaque do valor de retenções tributárias cabíveis.

9.13. 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.

9.14. 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.

9.15. A Administração deverá realizar consulta ao SICAF para:

9.15.1 verificar a manutenção das condições de habilitação exigidas;

9.15.2 identificar possível razão que impeça a participação em licitação/contratação, no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas.

9.16. 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.

9.17. 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.

9.18. 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.

9.19. 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

9.20. 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.

9.21. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice de Custo de Tecnologia da Informação - ICTI de correção monetária.

Forma de pagamento

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

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

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

9.25. 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.

9.26. 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

9.27. As cessões de crédito dependerão de prévia aprovação do Contratante.

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

9.27.2 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.

9.27.3 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.

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

9.28. O disposto nesta seção não afeta as operações de crédito de que trata a Instrução Normativa SEGES/MGI nº 82, de 21 de fevereiro de 2025, as quais ficam por esta regidas.

Reajuste

9.29. Os preços inicialmente contratados são fixos e irredutíveis no prazo de um ano contado da data do orçamento estimado, em 01/08/2025.

9.30. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

9.32. No caso de atraso ou não divulgação do índice de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

9.33. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

9.34. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

9.35. 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.

9.36. O reajuste será realizado por apostilamento.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

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 global total.

Forma de fornecimento

10.2. O fornecimento do objeto será integral.

Critérios de aceitabilidade de preços

10.3. Em se tratando de contratação para registro de preços, caso adotado o critério de julgamento de menor preço ou de maior desconto por grupo de itens, o critério de aceitabilidade de preços unitários máximos será:

10.3.1 Valores unitários: conforme tabela constante no item 1.1 deste Termo de Referência.

Exigências de habilitação

10.4. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:

Habilitação jurídica

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

10.6. empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

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

10.8. 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;

10.9. 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;

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

10.11. 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.

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

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

Habilitação fiscal, social e trabalhista

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

10.15. 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;

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

10.17. 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;

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

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

10.20. Caso o fornecedor seja considerado isento dos tributos 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.

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

Qualificação Econômico-Financeira

10.22. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;

10.23. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

10.24. balanço patrimonial, demonstração de resultados de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, já exigíveis e apresentados na forma da lei, comprovando, índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

10.25. Caso a empresa interessada 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 5% (cinco por cento) do valor total estimado da contratação.

10.26. Os indicadores fixados acima deverão ser atingidos em cada um dos dois últimos exercícios sociais, sob pena de inabilitação;

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

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

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

Qualificação Técnica

10.30. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado, ou pelo conselho profissional competente, quando for o caso.

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

10.31.1.1 Fornecimento de equipamentos, licenças, serviços e suporte similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação aos exigidos na quantidade mínima de 50% (cinquenta por cento) do solicitado, por meio da apresentação de um ou mais atestado(s) de capacidade técnica, expedido(s) por pessoa jurídica de direito público ou privado, idônea, estabelecida em território nacional, que comprove o fornecimento de serviços, bem como a prestação de garantia e suporte técnico em conformidade com as especificações descritas neste documento e anexos.

10.31. Serão admitidos, para fins de comprovação de quantitativo mínimo exigido, a apresentação e o somatório de diferentes atestados relativos a contratos executados de forma concomitante.

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

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

10.34. Será exigida Certificação NSE6 ou superior do prestador de serviços.

DO JULGAMENTO DAS PROPOSTAS E DO NÃO PARCELAMENTO DO OBJETO

10.35. A presente contratação será realizada sob o Sistema de Registro de Preços (SRP), adotando-se o critério de julgamento de menor preço por grupo de itens, conforme previsto no art. 33, inciso I, alínea “a”, da Lei nº 14.133, de 1º de abril de 2021, e no art. 10 do Decreto nº 11.462, de 31 de março de 2023.

10.36. A estrutura do grupo de itens decorre da indivisibilidade técnica e funcional da solução de segurança de rede, composta por equipamentos, licenças, serviços de suporte e implantação integrados, cuja interoperabilidade e garantia de funcionamento dependem do fornecimento conjunto pela mesma fabricante e integrador.

10.37. Assim, resta tecnicamente inviável a adjudicação por item isolado, uma vez que o fracionamento comprometeria a homogeneidade da solução, a continuidade do suporte técnico do fabricante, a segurança cibernética e a eficiência operacional da infraestrutura perimetral do Ministério dos Transportes.

10.38. Nos termos dos §§ 1º e 2º do art. 82 da Lei nº 14.133/2021, a adoção do critério de menor preço por grupo de itens fundamenta-se em vantagem técnica e econômica comprovada, assegurando padronização tecnológica, otimização de gestão contratual e economia de escala ao longo do ciclo de vida da solução.

10.39. O critério de aceitabilidade de preços unitários máximos será indicado no edital da licitação, garantindo transparência e rastreabilidade, em conformidade com o disposto no § 2º do art. 82 da referida Lei.

10.40. Dessa forma, a decisão pelo não parcelamento do objeto e pela adoção do julgamento por grupo de itens encontra-se devidamente justificada, atendendo aos princípios da eficiência, economicidade e vantajosidade para a Administração Pública, conforme a legislação vigente.

Disposições gerais sobre habilitação

10.41. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

10.42. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

10.43. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.44. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.45. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação, que corresponde ao valor máximo aceitável, é de **R\$ 17.808.591,00** (dezesete milhões, oitocentos e oito mil quinhentos e noventa e um reais), conforme custos unitários apostos na tabela do item 1.1.

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

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

11.3.1 em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

11.3.2 em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

11.3.3 serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou

11.3.4 poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

12. ADEQUAÇÃO ORÇAMENTÁRIA

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

12.2. A contratação será atendida pela seguinte dotação:

I) Gestão/Unidade: 390096 - Subsecretaria de Gestão Estratégica, Tecnologia e Inovação;

II) Fonte de Recursos: 1000000000;

III) Programa de Trabalho: 10.39101.26.126.0032.218T.0001;

IV) Elemento de Despesa: 339040;

V) Plano Interno: Não há;

VI) Ação orçamentária: 218T - Manutenção e Operação da Infraestrutura de Tecnologia da Informação da Administração Direta;

VII) Plano Orçamentário: 0000 - Manutenção de Operação da Infraestrutura de Tecnologia da Informação;

VIII) PTRES: 194808.

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

12.4. A indicação da dotação orçamentária fica postergada para o momento da assinatura do contrato ou instrumento equivalente.

13. DISPOSIÇÕES FINAIS

13.1. As informações contidas neste Termo de Referência não são classificadas como sigilosas.

Cronograma Físico Financeiro

13.2. Por se tratar de uma Ata de registro de preços, o Cronograma físico-financeiro será montado, a partir do momento em que houver a previsão do início da contratação.

14. Responsáveis

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

MARCEL VIEIRA DE CAMARGO

Integrante Administrativo



Assinou eletronicamente em 24/11/2025 às 16:44:25.

HENRIQUE ALCANTARA VELOSO MOTA

Integrante Requisitante



Assinou eletronicamente em 24/11/2025 às 16:37:38.

JULIO CESAR FERREIRA DA SILVA

Integrante Técnico



Assinou eletronicamente em 24/11/2025 às 16:41:17.

DIOGO DA FONSECA TABALIPA

Autoridade Máxima



Assinou eletronicamente em 24/11/2025 às 16:40:35.

Lista de Anexos

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

- Anexo I - ANEXO A - CADERNO DE ESPECIFICACOES TECNICAS-compactado.pdf (249.76 KB)
- Anexo II - ANEXO B - Modelo Proposta de Precos.pdf (278.55 KB)
- Anexo III - ANEXO C - Modelo de Ordem de Servico.pdf (244.7 KB)
- Anexo IV - ANEXO D - Termo de Compromisso de Manutencao do Sigilo.pdf (257.14 KB)
- Anexo V - ANEXO E - Termo de Ciencia.pdf (179.01 KB)



MINISTÉRIO DOS TRANSPORTES
SECRETARIA-EXECUTIVA
SUBSECRETARIA DE GESTÃO ESTRATÉGICA, TECNOLOGIA E INOVAÇÃO
COORDENAÇÃO-GERAL DE ENTREGA DE SERVIÇOS DE TECNOLOGIA
COORDENAÇÃO DE INFRAESTRUTURA TECNOLÓGICA

ANEXO A – CADERNO DE ESPECIFICAÇÕES TÉCNICAS

ITEM	PRODUTO/SERVIÇO	UNIDADE	QUANTIDADE
1	Solução de Proteção de Rede Perimetral – Período de 60 meses	UND	10
2	Sistema de Gerência Centralizada – Período de 60 meses	UND	05
3	Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede	UND	200
4	Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede	UND	4050

1.1. Especificações técnicas

1.1.1. Item 1 Solução de Proteção de Rede Perimetral

- 1.1.1.1.** A solução de segurança (NGFW) deve possuir a capacidade e as características abaixo:

1.1.1.1.1. Throughput de no mínimo, 15 (Quinze) Gbps, com as funcionalidades de Next Generation firewall(IPS e Application control habilitados simultaneamente), com padrão de tráfego empresarial ou similar.

1.1.1.1.2. Throughput de no mínimo, 12(Doze) Gbps, com as funcionalidades de Next Generation firewall, IPS, anti-malware e prevenção contra ameaças avançadas de dia-zero habilitadas e atuantes, conhecido como Threat Protection ou Threat Prevention);

1.1.1.1.3. Throughput de no mínimo, 10 (Dez) Gbps, para inspeção de tráfego SSL, considerando pelo menos funcionalidade de IPS sobre tráfego HTTPS/WEB.

1.1.1.1.4. O Throughput é a quantidade de tráfego que um único equipamento é capaz de encaminhar, não havendo soma entre os membros do cluster;

1.1.1.1.5. Suporte a, no mínimo, 7.500.000 (sete milhões e quinhentos mil) de conexões simultâneas;

1.1.1.1.6. Suporte a, no mínimo, 500.000 (quinhentos mil) novas conexões por segundo;

1.1.1.1.7. Armazenamento redundante de, no mínimo, de 480 GB SSD;

1.1.1.1.8. Deve possuir fontes de alimentação AC 100-240VAC redundantes e hot-swappable;

1.1.1.1.9. No mínimo, 8 (oito) interfaces de rede de GbE RJ-45;

1.1.1.1.10. No mínimo, 16 (Dezesseis) interfaces de rede de 1/10 Gbps SFP+/SFP acompanhado de seus respectivos Gbics do fabricante ofertado;

1.1.1.1.11. No mínimo, 4(Quatro) interfaces de rede de 25/10 SFP28/SFP+ slots acompanhado de seus respectivos Transceivers do fabricante ofertado;

1.1.1.1.12. No mínimo, 2(Duas) interfaces de rede de 40/100 Gbps QSFP+ slots acompanhado de seus respectivos Transceivers do fabricante ofertado;

1.1.1.1.13. No mínimo, 01 (uma) interface Gigabit dedicada para alta disponibilidade;

1.1.1.1.14. No mínimo, 01 (uma) interface Gigabit dedicada para Gerência;

1.1.1.1.15. 01 (uma) interface do tipo console ou similar;

1.1.1.1.16. Deverão ser licenciados para suportar, pelo menos, 1.000 (um mil) usuários de VPN de cliente.

1.1.1.1.17. VPN com capacidade de, pelo menos, 54 (cinquenta e quatro) Gbps de tráfego IPSec;

1.1.1.1.18. Suportar, no mínimo, 5 instâncias de firewall (cluster) e permitir a expansão, através de aquisição futura de licenças;

1.1.1.1.19. O Troughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.1.1.1.20. Todas as interfaces SFP+ fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores do tipo SR.

1.1.1.1.21. Não serão aceitos appliances virtualizados para os firewalls, somente equipamentos físicos.

1.1.1.2. Funcionalidades do Firewall:

1.1.1.2.1. As funcionalidades de firewall devem possuir a capacidade e as características abaixo:

1.1.1.2.2. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.1.2.3. Deve possibilitar a elaboração de políticas baseadas em geolocalização, permitindo o bloqueio de tráfego proveniente de determinado(s) país(es);

1.1.1.2.4. Deve permitir a exibição dos países de origem e destino nos registros de acesso;

1.1.1.2.5. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

1.1.1.2.6. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

1.1.1.2.7. Controle, inspeção e de-criptografia de SSL por política para tráfego de saída;

1.1.1.2.8. Deve ser possível realizar um espelhamento do tráfego de-criptografado;

1.1.1.2.9. Deve de-criptografar tráfego de saída em conexões negociadas com TLS 1.2 e TLS 1.3;

1.1.1.2.10. A inspeção SSL deve ser compatível com HTTP3. Tal inspeção é essencial uma vez que uma grande quantidade de sítios públicos está utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos;

1.1.1.2.11. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.1.1.2.12. A plataforma deve ser otimizada para análise de conteúdo de aplicações em Camada 7 (Web Application Firewall);

1.1.1.2.13. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

1.1.1.2.14. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.1.2.15. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

1.1.1.3. Deve suportar os seguintes tipos de NAT e Roteamento:

1.1.1.3.1. NAT dinâmico (Many-to-1), NAT estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.1.3.2. Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing);

1.1.1.3.3. Deve suportar atuar como proxy reverso para aplicações Web que utilizem protocolos HTTP e HTTPS;

1.1.1.3.4. Para IPv4, deve suportar roteamento estático e dinâmico (RIP V1, V2, OSPF e BGPv4) Para IPv6, deve suportar roteamento estático e dinâmico (RIPv6, BGP4+, OSPFv3);

1.1.1.3.5. Deve suportar NAT64

1.1.1.3.6. Deverá suportar roteamento estático e dinâmico;

1.1.1.3.7. Deve estar equipado com ferramenta de monitoração de pacotes de rede tipo sniffer para acompanhamento e visualização de tráfego de rede em tempo real, não sendo aceito soluções que fazem a gravação do tráfego para posterior abertura e análise, inclusive com a capacidade de aplicação de filtros personalizados;

1.1.1.3.8. O Firewall deve ter a capacidade de operar de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

1.1.1.3.9. Deve possuir sistema de monitoramento em tempo real do hardware via interface gráfica, interface Web HTTPS e linha de comando CLI;

1.1.1.3.10. Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

1.1.1.3.11. Deverá suportar sFlow ou NetFlow;

1.1.1.3.12. Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

1.1.1.3.13. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

1.1.1.3.14. Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança.

1.1.1.4. Funcionalidades de Prevenção de Ataques:

1.1.1.4.1. Deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão.

1.1.1.4.2. Deverá oferecer a capacidade de determinar políticas conforme o tempo, isto é, estabelecer normas para horários ou intervalos específicos (dia, mês, ano, dia da semana e hora);

1.1.1.4.3. A criação de políticas por agrupamentos de usuários, endereços IP, redes ou áreas de segurança deverá ser possível;

1.1.1.4.4. Deve ter a competência para criar políticas baseadas na visibilidade e controle de quem usa quais URLs, integrando com serviços de diretório, Active Directory e banco de dados local;

1.1.1.4.5. A identificação através do Active Directory deve habilitar SSO, de modo que os usuários não tenham que fazer login novamente na rede para passar pelo firewall;

1.1.1.4.6. Deve suportar a criação de políticas baseadas no controle por URL e categoria de URL;

1.1.1.4.7. Deve ter categorias de URLs pré-estabelecidas pelo fabricante que podem ser atualizadas a qualquer momento;

1.1.1.4.8. Deve ter no mínimo 50 categorias de URLs;

1.1.1.4.9. Deve contar com a função para excluir URLs do bloqueio;

1.1.1.4.10. Deverá permitir a personalização da página de bloqueio;

1.1.1.4.11. Deve possibilitar a limitação do acesso a canais específicos do YouTube, permitindo a configuração de uma lista de canais permitidos ou uma lista de canais bloqueados;

1.1.1.4.12. Deve impedir o acesso a conteúdo inadequado quando se utiliza a pesquisa em sites como Google, Bing e Yahoo, independentemente da opção Safe Search estar ativada no navegador do usuário;

1.1.1.4.13. Deve contar com recurso de prevenção contra phishing de credenciais, analisando quais estão sendo submetidas em sites externos, e ainda bloquear ou alertar o usuário;

1.1.1.4.14. Deve proporcionar a opção de estabelecer uma cota diária de uso web baseada em categoria, podendo estabelecer a cota com base, pelo menos, no tempo de uso e volume de tráfego;

1.1.1.4.15. Deverá ser possível bloquear tráfego HTTP POST, método usado para envio de informação a um website específico;

1.1.1.4.16. Deverá ser capaz de filtrar e remover Java applets, ActiveX e cookies do tráfego web inspecionado;

1.1.1.4.17. Deve possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados mal-intencionados;

1.1.1.4.18. A filtragem de tráfego de vídeo com base na categoria e até mesmo no identificador de um canal do YouTube, por exemplo, deve ser possível;

1.1.1.4.19. Além de suportar Web Proxy explícito, deverá permitir Proxy Web transparente;

1.1.1.4.20. Deverá estar orientado à proteção de redes;

1.1.1.4.21. Deverá permitir funcionar em modo transparente, porta espelhada e gateway das redes protegidas.

1.1.1.4.22. Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente.

1.1.1.4.23. Deverá permitir a criação de padrões de ataque manualmente.

1.1.1.4.24. Deverá possuir integração à plataforma de segurança.

1.1.1.4.25. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques.

1.1.1.4.26. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web.

1.1.1.4.27. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.

1.1.1.4.28. Deverá possuir análise de protocolos.

1.1.1.4.29. Deverá possuir detecção de anomalias.

1.1.1.4.30. Deverá possuir detecção de ataques de RPC (Remote Procedure Call).

1.1.1.4.31. Deverá possuir proteção contra-ataques de Windows ou NetBios.

1.1.1.4.32. Deverá possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol).

1.1.1.4.33. Deverá possuir proteção contra-ataques DNS (Domain Name System).

1.1.1.4.34. Deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin.

1.1.1.4.35. Deverá possuir proteção contra-ataques de ICMP (Internet Control Message Protocol).

1.1.1.4.36. Deverá possuir métodos de notificação de detecção de ataques.

1.1.1.4.37. Deverá possuir alarmes na console de administração.

1.1.1.4.38. Deverá possuir alertas via correio eletrônico.

1.1.1.4.39. Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.

1.1.1.4.40. Deverá ter a capacidade de resposta/logs ativa a ataques.

1.1.1.4.41. Deverá ter a capacidade de detectar e bloquear ameaças avançadas, como malware, ransomware e outras ameaças que os firewalls tradicionais podem não ser capazes de lidar. Isso é muitas vezes alcançado através da integração com outras tecnologias de segurança, como sistemas de prevenção de intrusões (IPS), proteção avançada contra malware (AMP) e sandboxing;

- 1.1.1.4.42. Deverá prover a terminação de sessões via TCP resets.
- 1.1.1.4.43. Deverá armazenar os logs de sessões.
- 1.1.1.4.44. Deverá mitigar os efeitos dos ataques de negação de serviços.
- 1.1.1.4.45. Deverá permitir a criação de assinaturas personalizadas.
- 1.1.1.4.46. Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion.
- 1.1.1.4.47. Deverá suportar verificação de ataque na camada de aplicação.
- 1.1.1.4.48. Deverá suportar verificação de tráfego em tempo real, via aceleração de hardware.
- 1.1.1.4.49. Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset.

1.1.1.5. Funcionalidades de Controle de Qualidade do Serviço:

- 1.1.1.5.1. Suportar a criação de políticas de QoS por:
- 1.1.1.5.2. Endereço de origem, endereço de destino e por porta;
- 1.1.1.5.3. O QoS deve possibilitar a definição de classes por:
- 1.1.1.5.4. Banda garantida, banda máxima e fila de prioridade;
- 1.1.1.5.5. Disponibilizar estatísticas RealTime para classes de QoS;
- 1.1.1.5.6. Funcionalidades de VPN:
- 1.1.1.5.7. Suportar VPN Site-to-Site e Cliente-To-Site;
- 1.1.1.5.8. Suportar IPSEC VPN;
- 1.1.1.5.9. A VPN IPSEC deve suportar:
- 1.1.1.5.10. 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES

128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

1.1.1.6. Suportar SSL VPN o qual deve:

1.1.1.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional (Windows e Linux) do equipamento ou por meio de interface WEB;

1.1.1.6.2. Permitir que o usuário realize conexão através de dispositivos mobile (Android e IOS) através de um cliente instalado do fabricante ofertado.

1.1.1.6.2.1. Por questões de segurança, não serão aceitos cliente mobile de terceiros;

1.1.1.6.3. A funcionalidades de VPN de cliente devem ser atendidas com ou sem o uso de agente;

1.1.1.6.4. Deve ser capaz de informar se a senha do usuário da VPN de cliente autenticado via Microsoft Active Directory expirou e permitir que o usuário faça a troca da senha;

1.1.1.6.5. Atribuição de endereço IP nos clientes remotos de VPN;

1.1.1.6.6. Atribuição de DNS nos clientes remotos de VPN;

1.1.1.6.7. A solução ofertada deve suportar a tecnologia de VPN Dinâmica entre as filiais (ADVPN);

1.1.1.6.8. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

1.1.1.6.9. Suportar leitura e verificação de CRL (certificate revocation list);

1.1.1.6.10. O agente de VPN de cliente client-to-site deve ser compatível com pelo menos: Windows, Linux e Mac OS X.;

1.1.1.6.11. Deve suportar duplo fator de autenticação para a conexão VPN;

1.1.1.6.12. Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN.

1.1.1.7. Suportar SD-WAN;

1.1.1.7.1. Não deve limitar número de links a serem balanceados.

1.1.1.7.2. Realizar balanceamento de tráfego de saída entre os links de Wan primários;

1.1.1.7.3. Permitir que a escolha do link WAN de saída seja influenciada por regras definidas pelo administrador de rede. As regras devem permitir ao menos um dos parâmetros a seguir ou combinação destes:

1.1.1.7.3.1. Endereço IP de origem e/ou destino;

1.1.1.7.3.2. Subredes de origem e/ou destino;

1.1.1.7.3.3. Métricas de Jitter, latência e perda de pacotes por aplicação;

1.1.1.7.3.4. Status da porta de WAN primários (UP ou DOWN);

1.1.1.7.4. Deve reconhecer e respeitar no tráfego SD-Wan, para o teste de saúde dos links, o atributo DSCP "Differentiated Services Code Point", para aferição mais precisa conforme criticidade das aplicações.

1.1.1.7.5. Toda a comunicação Wan deve trafegar em um túnel VPN ponto-a-ponto estabelecido dinamicamente entre os PONTOS DE PRESENÇA.

1.1.1.7.6. Suportar o protocolo de tunelamento GRE (General Routing Encapsulation - RFC 2784);

1.1.1.7.7. A topologia da rede WAN deve ser dentre outras possíveis, a de malha completa (full mesh);

1.1.1.7.8. O estabelecimento do túnel VPN entre os pontos de presença pode inicialmente ser orientado pelo concentrador, mas o tráfego de dados

após o estabelecimento do túnel deve ser realizado diretamente entre os integrantes do túnel, sem consumir throughput do concentrador;

1.1.1.7.9. Tratar o tráfego SD-Wan das aplicações críticas respeitando e aplicando as tags DSCPs das mesmas.

1.1.1.7.10. A solução de SD-WAN deverá ser integrada no próprio appliance de NGFW.

1.1.1.7.11. Permitir a monitoração dos links SD-Wan através de protocolos: ping, http, tcp-echo e udp-echo;

1.1.1.7.12. Permitir a monitoração dos links SD-Wan através do Protocolo IP nas versões 4 e 6;

1.1.1.7.13. Permitir a monitoração dos links SD-Wan combinando fatores de saúde podendo variar entre: tempo de checagem, número de checagens antes de declarar o link como não operacional e número de checagens antes de declarar o link como operacional novamente;

1.1.1.7.14. Quando ambos os pontos de extremidade dos túneis SD-WAN estiverem ativos, deve haver a duplicação de pacotes (PD) para manter a experiência dos usuários mesmo em condição de perda de pacotes. A duplicação de pacotes deve criar uma cópia do fluxo de tráfego do aplicativo e a enviar em ambos os túneis disponíveis, que está orientado ao mesmo destino.

1.1.1.7.15. O dispositivo de SD-WAN deve utilizar "Forward Error Correction" (FEC) habilitado, para permitir que aplicações sensíveis à perda de pacotes não sejam impactadas em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho.

1.1.1.8. Prevenção de Ameaças Avançadas (zero day)

1.1.1.8.1. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado, ou analisado dinamicamente com mecanismo de IA em ambiente controlado;

1.1.1.8.2. Deve ser capaz de enviar para análise, arquivos tipo Executáveis, DLLs, Arquivos de Código e MSI;

1.1.1.8.3. A solução deve detectar e bloquear em tempo real (inline) os artefatos maliciosos desconhecidos (zero day) no próprio GW, após validação pelo ambiente Cloud de Sandbox.

1.1.2. Item 2 - Sistema de Gerência Centralizada

1.1.2.1. Deve prover gestão centralizada dos equipamentos e ser necessariamente do mesmo fabricante do NGFW.

1.1.2.2. Por console de gerência, entende-se as licenças de software necessárias para esta funcionalidade.

1.1.2.3. Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização: VMware ESX/ESXi 6.7, Proxmox e Microsoft Hyper-V.

1.1.2.4. Deverá possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 60 (sessenta) meses.

1.1.2.5. Deverá possuir a capacidade de receber pelo menos 20 GB de logs diários.

1.1.2.6. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.

1.1.2.7. Permitir acesso concorrente de administradores.

- 1.1.2.8.** Deverá possuir autenticação de usuários para acesso à plataforma via LDAP e RADIUS.
- 1.1.2.9.** Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores.
- 1.1.2.10.** Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.
- 1.1.2.11.** Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora.
- 1.1.2.12.** Deve registrar as ações efetuadas por quaisquer usuários.
- 1.1.2.13.** O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação.
- 1.1.2.14.** O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e AntiSpyware.
- 1.1.2.15.** O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL.
- 1.1.2.16.** Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).
- 1.1.2.17.** O servidor de gerência deve ser hospedado em um equipamento independente, não exercendo funções de firewall.
- 1.1.2.18.** A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.
- 1.1.2.19.** A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.
- 1.1.2.20.** Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas.

- 1.1.2.21.** Deverá possuir mecanismos de apagamento automático para logs antigos.
- 1.1.2.22.** Deverá permitir importação e exportação de relatórios.
- 1.1.2.23.** Deverá ter a capacidade de criar relatórios no formato HTML.
- 1.1.2.24.** Deverá ter a capacidade de criar relatórios em formato PDF.
- 1.1.2.25.** Deverá permitir exportar os logs no formato CSV.
- 1.1.2.26.** Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.
- 1.1.2.27.** Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.
- 1.1.2.28.** Suportar o padrão SAML para autenticação do usuário administrador.
- 1.1.2.29.** Deverá estar licenciada para a quantidade de equipamentos a serem gerenciados.
- 1.1.2.30.** Deverá Suportar até 20 GB de logs por dia;
- 1.1.2.31.** Deverá possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 60 (sessenta) meses.
- 1.1.2.32.** Deverá integrar e gerenciar todos os ativos dos itens do objeto;
- 1.1.2.33.** Deverá permitir instalar políticas pontualmente em seus gateways gerenciados, no gateway específico, não sendo aceito soluções com aplicações de políticas generalizadas para todo o parque gerenciado;
- 1.1.2.34.** Deverá permitir instalar políticas "diferenciais", ou seja: apenas as alterações novas devem ser enviadas para os gateways selecionados, deixando inalterada a parte remanescente já configurada e em uso. Não sendo aceito soluções com aplicações de políticas generalizadas para todo o parque gerenciado.
- 1.1.2.35.** Caso a Console de Operação da Solução de Gerenciamento Centralizado seja baseada em tecnologias descontinuadas, e.x Java, não será aceito, devendo ser

fornecido método alternativo para garantia da integridade do Ambiente de Segurança e protegido.

1.1.3. Item 3 – Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede

- 1.1.3.1.** A Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas;
- 1.1.3.2.** A solução deve estar licenciada para um total de 100 (cem) usuários;
- 1.1.3.3.** A Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede deve prover um método de controlar o acesso identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust;
- 1.1.3.4.** A Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão;
- 1.1.3.5.** A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário;
- 1.1.3.6.** Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem;
- 1.1.3.7.** A solução deve ser escalável até 500 agentes;
- 1.1.3.8.** O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante;
- 1.1.3.9.** Deve ser compatível com pelo menos os seguintes sistemas operacionais: Microsoft Windows: 7 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11 (64 bits), Microsoft Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022, Mac

OS X: versões 13, 12, 11 e 10.15, Linux: Ubuntu 18.04 e posterior, Debian 11 e posterior, CentOS Stream 8, CentOS 7.4 e posterior, RedHat 7.4 e posterior, Fedora 36 e posterior;

- 1.1.3.10.** A Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel;
- 1.1.3.11.** A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.3;
- 1.1.3.12.** Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários;
- 1.1.3.13.** A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso;
- 1.1.3.14.** Deve ser possível revogar o certificado de um agente por meio da console central;
- 1.1.3.15.** O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso;
- 1.1.3.16.** No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão;
- 1.1.3.17.** Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional;

- 1.1.3.18.** A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até cinco dias anteriores ao ocorrido;
- 1.1.3.19.** Deve ser possível determinar para quais funcionalidades o log deve estar habilitado e permitir que esses dados sejam enviados para a console central;
- 1.1.3.20.** Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, debug;
- 1.1.3.21.** Deve ser possível exportar os logs diretamente a nível de agente;
- 1.1.3.22.** Deve ser possível exigir uma senha para desconectar o agente da console central;
- 1.1.3.23.** Deve existir a possibilidade de restringir o usuário de realizar backup da configuração do agente;
- 1.1.3.24.** Deve ser possível evitar que o usuário realize um shutdown do agente após estar registrado à console central;
- 1.1.3.25.** Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes. Deve ser possível ainda atribuir tags aos endpoints de acordo com o índice de comprometimento detectado pela solução de consolidação de logs, desde que haja licenciamento instalado para tal;
- 1.1.3.26.** Deve ser possível configurar o agente para usar Proxy;
- 1.1.3.27.** O agente deve permitir a configuração local via XML (eXtensible Markup Language);
- 1.1.3.28.** Deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central;
- 1.1.3.29.** Este convite deve gerar um código a ser inserido no passo de registro do agente e deve ser possível ainda adicionar um passo de verificação da autenticação do usuário, podendo associar a autenticação via base de dados local, LDAP e SAML;

- 1.1.3.30.** Deverá ser possível enviar uma notificação por e-mail contendo o código de registro para os usuários finais informados, bem como um link para download do instalador do agente;
- 1.1.3.31.** Deve ser possível especificar a validade do código de registro;
- 1.1.3.32.** A console central de agentes deve dispor de métodos para determinar se um usuário está on-net ou off-net, ou seja, dentro ou fora da rede corporativa.
- 1.1.3.33.** Deve ser possível ainda criar perfis de configurações distintos para os usuários on-net e off-net;
- 1.1.3.34.** A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4;
- 1.1.3.35.** Deve ser possível agrupar agentes em grupos;
- 1.1.3.36.** Deve ser possível atribuir grupos de agentes a perfis de políticas específicos;
- 1.1.3.37.** Deve ser possível atribuir um nível de prioridade a um perfil de política visando priorizar qual política será utilizada caso um grupo de agentes esteja associado a mais de um perfil de política;
- 1.1.3.38.** A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA;
- 1.1.3.39.** O proxy de acesso deve atuar como proxy reverso para aplicações baseadas em HTTP, HTTPS, RDP, SMB, CIFS, SSH, SMTP, SMTPS, IMAP, IMAPS, POP3 e POP3S;

- 1.1.3.40.** Para aplicações HTTP e HTTPS deve ser possível realizar um balanceamento de carga entre os servidores cadastrados usando algoritmos como round robin, por peso, baseado no host field do cabeçalho HTTP ou baseado em disponibilidade do servidor;
- 1.1.3.41.** Para regras de encaminhamento de tráfego TCP, deve ser possível vincular o servidor com um FQDN visando ofuscar o endereço IP privado do servidor.
- 1.1.3.42.** Deste modo, o agente deve manipular o host file do endpoint visando criar entradas DNS;
- 1.1.3.43.** Deve ser possível definir um pool de IPs no proxy de acesso como IPs de origem para comunicação interna com as aplicações privadas;
- 1.1.3.44.** A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa;
- 1.1.3.45.** Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas;
- 1.1.3.46.** As regras de conformidade devem gerar tags que são sincronizadas entre os elementos da Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede visando controlar a postura de um determinado endpoint diretamente no proxy de acesso;
- 1.1.3.47.** A postura deve ser monitorada continuamente para que, caso ocorra uma alteração, o proxy de acesso termine e passe a bloquear a conexão em desacordo com as regras de compliance definidas;
- 1.1.3.48.** Deve ser possível construir tags com verificações no endpoint, as quais podem variar de acordo com o suporte ao sistema operacional, tais como se o endpoint está logado no domínio, versão do sistema operacional, chave de registro, processo, nível de vulnerabilidade, CVEs, arquivos existentes em um caminho específico e até

mesmo se o antivírus está instalado e sendo executado, além de ser possível validar se as assinaturas estão atualizadas;

1.1.3.49. A console central deve permitir exportar e importar tags entre sistemas diferentes por meio de um arquivo JSON;

1.1.3.50. Deve ser possível verificar quais endpoints estão associadas com cada tag;

1.1.3.51. Deve ser possível criar regras no proxy de acesso determinando se um dispositivo necessita estar de acordo com uma ou mais de uma tag simultaneamente, caso a política possua vínculo com diversas tags;

1.1.3.52. Deve ser possível criar regras no proxy de acesso vinculando interface de origem, IP de origem, IP de destino, servidor ZTNA, tag ZTNA, grupo de usuários ou usuário;

1.1.3.53. Para validação da autenticação dos usuários em conjunto com as regras de proxy de acesso, a solução deve suportar SAML, LDAP, Radius ou base de dados local;

1.1.3.54. Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais;

1.1.3.55. Deve possibilitar aos usuários definirem suas identidades mediante inserção manual, vínculo com LinkedIn, Google ou Salesforce, podendo ainda notificá-los para que esse vínculo possa ser realizado;

1.1.3.56. A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional;

1.1.3.57. Deverá ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows;

1.1.3.58. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente;

- 1.1.3.59.** Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos;
- 1.1.3.60.** Caso não seja possível aplicar um patch automático para corrigir uma vulnerabilidade, requerendo assim um patch manual, deve ser possível excluir essa aplicação da verificação de compliance;
- 1.1.3.61.** Deve ser possível excluir determinadas aplicações da verificação de compliance e até mesmo desabilitar o patch automático;
- 1.1.3.62.** O agente deve dispor de um sistema de notificação do tipo popup visando alertar o usuário;
- 1.1.3.63.** Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, severidade, bem como o CVE correspondente;
- 1.1.3.64.** Deve suportar a criação de várias versões de pacotes de instalação;
- 1.1.3.65.** As vulnerabilidades encontradas devem ser exibidas diretamente no agente com um link para análise de mais detalhes, englobando nome da vulnerabilidade, severidade, produtos afetados, CVE IDs, descrição, informação do fabricante do software e, quando disponível, link para download do patch no site público do fabricante do software;
- 1.1.3.67.** Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas, bem como disponibilizar ainda a possibilidade de aplicar a remediação imediatamente;
- 1.1.3.68.** Deve possuir módulo para execução de filtro web a nível de endpoint mediante uso do agente local, realizando a filtragem diretamente no endpoint, podendo ainda ser possível bloquear, permitir, alertar ou monitorar o tráfego web com base na categoria de URL ou filtro de URL customizado;
- 1.1.3.69.** O agente deve realizar consultas online ao centro de inteligência do próprio fabricante para determinar a categoria de uma determinada URL visando aplicar o controle de acesso à Internet;

- 1.1.3.70. Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar;
- 1.1.3.71. O agente para Windows deve permitir inspeção de tráfego HTTPS mediante instalação de plugin disponibilizado pelo mesmo fabricante do agente, o qual deve ser compatível com Google Chrome, Mozilla Firefox e Microsoft Edge;
- 1.1.3.72. Deve ser possível verificar as violações de filtro web diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário;
- 1.1.3.73. Deve ser possível determinar quando o filtro web entrará em ação no agente, se o mesmo deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa;
- 1.1.3.74. Deve ser possível configurar o proxy de acesso para atuar como CASB (Cloud Access Security Broker) em linha, inline do inglês, visando controlar o acesso a aplicações SaaS;
- 1.1.3.75. O proxy de acesso deve manter uma base de aplicações dinâmica, a qual deve ser compartilhada pelo centro de inteligência do fabricante da solução;

1.1.4. Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede

- 1.1.4.1. Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas Vmware ESXi, AWS e Microsoft Azure;
- 1.1.4.2. Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN do órgão;
- 1.1.4.3. Deve suportar variadas soluções de Wi-Fi do mercado, tais como: Aruba, Ruckus, Cisco, Fortinet, Aerohive e Enterasys, pelo menos;
- 1.1.4.4. A solução deve suportar capacidade de expansão para até 1500 endpoints simultâneos, sem demandar do cliente a troca do hardware/VM;

- 1.1.4.5.** A solução deve estar licenciada para operação com, pelo menos, 1500 endpoints conectados simultaneamente;
- 1.1.4.6.** A solução deve ser entregue em alta disponibilidade;
- 1.1.4.7.** A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);
- 1.1.4.8.** Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;
- 1.1.4.9.** A licença contemplada deverá suportar todas as características exigidas neste termo de referência;
- 1.1.4.10.** A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence;
- 1.1.4.11.** Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;
- 1.1.4.12.** Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:
 - 1.1.4.12.1.** Consultas em DHCP Fingerprint;
 - 1.1.4.12.2.** Consultas via protocolos HTTP/HTTPS;
 - 1.1.4.12.3.** Consultas via protocolo SNMP;
 - 1.1.4.12.4.** Consultas via protocolo SSH;
 - 1.1.4.12.5.** Consultas via protocolo Telnet;
 - 1.1.4.12.6.** Consultas de portas TCP;
 - 1.1.4.12.7.** Consultas de portas UDP;
 - 1.1.4.12.8.** MAC OUI;

1.1.4.12.9. Consultas via protocolo WMI;

1.1.4.12.10. Protocolo ONVIF;

1.1.4.12.11. Protocolo NetFlow;

1.1.4.12.12. Base assinaturas pré-definidas;

1.1.4.13. A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:

1.1.4.13.1. Endereço MAC;

1.1.4.13.2. Endereço IP;

1.1.4.13.3. Sistema operacional;

1.1.4.13.4. Nome do host;

1.1.4.13.5. Horário de conexão;

1.1.4.13.6. Usuário conectado;

1.1.4.13.7. Localização.

1.1.4.14. A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:

1.1.4.14.1. Android;

1.1.4.14.2. Apple iOS para iPhone, iPod e iPad;

1.1.4.14.3. Chrome OS;

1.1.4.14.4. Linux;

1.1.4.14.5. MacOS X;

1.1.4.14.6. Windows 7, 8 e 10;

1.1.4.15. Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;

- 1.1.4.16.** Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;
- 1.1.4.17.** Deve permitir a recategorização periódica de dispositivos;
- 1.1.4.18.** Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;
- 1.1.4.19.** A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;
- 1.1.4.20.** A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;
- 1.1.4.21.** A solução deve suportar RADIUS Change of Authorization;
- 1.1.4.22.** A solução deve suportar MAC Address Bypass;
- 1.1.4.23.** A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;
- 1.1.4.24.** A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinamicamente o acesso à rede;
- 1.1.4.25.** Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;
- 1.1.4.26.** Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, email, telefone), características da máquina (asset tag, hostname), localidade e horário;
- 1.1.4.27.** A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;
- 1.1.4.28.** A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;

- 1.1.4.29.** A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;
- 1.1.4.30.** A solução deve possuir ferramenta que permita a criação de credenciais para eventos;
- 1.1.4.31.** Deve permitir a definição de complexidade da senha dos usuários visitantes;
- 1.1.4.32.** Deve ser possível definir um período de validade para as contas de usuários visitantes;
- 1.1.4.33.** Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;
- 1.1.4.34.** A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;
- 1.1.4.35.** Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;
- 1.1.4.36.** A solução deve vincular o login do visitante à máquina utilizada no acesso;
- 1.1.4.37.** Deve suportar a validação de credenciais:
- 1.1.4.37.1. Em base local interna à ferramenta;
 - 1.1.4.37.2. Em servidores RADIUS;
 - 1.1.4.37.3. Em servidores LDAP.
- 1.1.4.38.** A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter;
- 1.1.4.39.** A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;
- 1.1.4.40.** Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;

- 1.1.4.41.** A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;
- 1.1.4.42.** Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;
- 1.1.4.43.** Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;
- 1.1.4.44.** Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução;
- 1.1.4.45.** A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;
- 1.1.4.46.** Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;
- 1.1.4.47.** A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade;
- 1.1.4.48.** Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;
- 1.1.4.49.** Tanto para IoTs quanto para estações de trabalho, se configurado, não devem ter qualquer acesso à rede de produção enquanto não forem inspecionados e identificados;
- 1.1.4.50.** Se um dispositivo não passar os testes de conformidade, deve ser possível:
- 1.1.4.50.1. Não forçar a remediação;
 - 1.1.4.50.2. Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;

1.1.4.50.3. Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena;

1.1.4.51. A solução deve permitir verificações de conformidade em endpoints que façam uso do sistema operacional:

1.1.4.51.1. Windows 7;

1.1.4.51.2. Windows 8;

1.1.4.51.3. Windows 10;

1.1.4.51.4. MacOS;

1.1.4.51.5. Linux.

1.1.4.52. Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:

1.1.4.52.1. Presença de software de anti-vírus instalado e em execução;

1.1.4.52.2. Versão do sistema operacional;

1.1.4.52.3. Nome de domínio do Active Directory ao qual a estação Windows pertença;

1.1.4.52.4. Serviços em execução para estações Windows;

1.1.4.52.5. Informações sobre um determinado certificado digital em estações Windows;

1.1.4.52.6. Registros ou chaves de registro para estações Windows;

1.1.4.52.7. Processos em execução para estações Windows, Linux e MacOS;

1.1.4.52.8. Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;

1.1.4.52.9. Pacotes instalados em estações Linux e MacOS.

1.1.4.53. A solução deve ser capaz de monitorar quando um serviço requerido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança;

1.1.4.54. Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;

1.1.4.55. Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos:

1.1.4.55.1. Programas de gerenciamento e distribuição de software;

1.1.4.55.2. GPO do Active Directory;

1.1.4.55.3. Captive Portal;

1.1.4.56. Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;

1.1.4.57. O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos;

1.1.4.58. Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;

1.1.4.59. A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;

1.1.4.60. No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de email e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance;

1.1.4.61. A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;

- 1.1.4.62.** Deve suportar integração com soluções de patching;
- 1.1.4.63.** Deve suportar integração com soluções de análise de vulnerabilidades;
- 1.1.4.64.** A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;
- 1.1.4.65.** A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;
- 1.1.4.66.** A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;
- 1.1.4.67.** A solução deve armazenar os eventos internamente e permitir que sejam exportados;
- 1.1.4.68.** A solução deve permitir a exportação dos eventos através de syslog;
- 1.1.4.69.** Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;
- 1.1.4.70.** A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso;
- 1.1.4.71.** Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;
- 1.1.4.72.** Suportar integração com soluções de segurança de fabricantes como: Fortinet, Palo Alto, FireEye, etc, para correlacionar alertas de segurança e restringir, isolar ou bloquear dispositivos comprometidos que estejam conectados na rede, reduzindo assim o tempo de contenção de ameaças;
- 1.1.4.73.** Suportar método genérico para integração de dispositivos, usando o recebimento, envio, análise e interpretação de mensagens do tipo syslog;
- 1.1.4.74.** Deve possibilitar o rastreo de dispositivos, notificando a localização dos mesmos quando se conectarem à rede;

1.1.4.75. Caso o CONTRATANTE não tenha solução de logs compatível com o NAC ofertado, cabe ao fornecedor incluí-la na proposta, sem ônus, considerando licenciamento e/ou hardware adequado para retenção dos logs;

1.1.4.76. Dentre os relatórios disponibilizados pela solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e rogues;



MINISTÉRIO DOS TRANSPORTES

SECRETARIA-EXECUTIVA

SUBSECRETARIA DE GESTÃO ESTRATÉGICA, TECNOLOGIA E INOVAÇÃO

COORDENAÇÃO-GERAL DE ENTREGA DE SERVIÇOS DE TECNOLOGIA

COORDENAÇÃO DE INFRAESTRUTURA TECNOLÓGICA

ANEXO - B

MODELO DE PROPOSTA DE PREÇOS

(em papel timbrado da empresa)

Ao

Ministério dos Transportes

Coordenação-Geral de Licitações e Contratos

Esplanada dos Ministérios, Bloco "R" - Térreo - Sala 5 - Ala Oeste - Edifício Anexo

CEP: 70.044-902 Brasília - DF

Referência: Pregão Eletrônico nº ____/____.

- 1.1. Proposta que faz a empresa _____, inscrita no CNPJ nº _____ e inscrição estadual nº _____, estabelecida no(a) _____, para eventual contratação de empresa especializada para o Registro de Preços para a eventual contratação de empresa especializada no fornecimento de Solução de Proteção de Rede Perimetral – Período de 60 meses, da empresa Fabricante Fortinet, incluída a Subscrição de todas as Licenças do Conjunto de Funcionalidades, serviços de implantação e transferência de tecnologia, garantia de atualização contínua do sistema operacional e suporte técnico de instalação durante o período de garantia, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

PLANILHA DE PROPOSTA DE PREÇOS

DOS VALORES DOS SERVIÇOS

Grupo	Item	Descrição	Unidade	Quantidade	Valor Unit. R\$	Valor Total (60 meses) R\$
1	1	Solução de Proteção de Rede Perimetral – Período de 60 meses	Unidade	10		
	2	Sistema de Gerência Centralizada – Período de 60 meses	Unidade	05		
	3	Extensão do Conjunto de Funcionalidades - Controle de acesso com Proteção do acesso remoto à rede	Unidade	200		
	4	Extensão do Conjunto de Funcionalidades - Gestão de ativos com detecção de dispositivos conectados à rede	Unidade	4050		
VALOR TOTAL (R\$)						

Nota: A proposta deverá ser apresentada de documentação técnica da solução e o link de internet em que se encontra hospedada a documentação necessária que possibilite a verificação dos requisitos técnicos/funcionais da solução.

DA SOLUÇÃO OFERTADA

Item	Descrição	Nome Específico do Software / Fabricante	Código de identificação unívoca (Part Number / SKU)	Link
1				
2				
3				
4				

SOFTWARE: (deverá ser informado, **obrigatoriamente**, o detalhamento dos softwares a serem fornecidos, quando for o caso, acompanhados dos respectivos *datasheets*)

Nome do Software: _____ Part Number/SKU: _____

Nome do Fabricante: _____

Procedência: 1. Nacional [] 2. Importado: []

Sítio na WEB do Fabricante: _____

Responsável: _____ Telefone Contato: _____

1) Dados da Proposta:

Valor Total: R\$ _____ (**VALOR POR EXTENSO**).

2) Validade da Proposta: 60 (sessenta) dias, a contar da data de sua apresentação.

3) Informamos, por oportuno, que nos preços apresentados acima já estão computados todos os custos necessários decorrentes da prestação dos serviços, bem como já incluídos todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, seguros, deslocamentos de pessoal e quaisquer outros que incidam direta ou indiretamente.

4) Dados da empresa:

a) Razão Social: _____

b) CNPJ (MF) nº _____

c) Inscrição Estadual nº: _____

d) Endereço: _____

e) Telefone: _____ Fax: _____ e-mail: _____

f) Cidade: _____ Estado: _____

g) CEP: _____

h) Representante(s) legal(is) com poderes para assinar o contrato:

a. Nome: _____

b. Cargo: _____

i) Dados Bancários:

a. Banco: _____

b. Agência: _____

c. Conta Corrente: _____

j) Dados para Contato:

a. Nome: _____

b. Telefone/Ramal: _____

Declaramos, para todos os fins e efeitos legais, aceitar, irrestritamente, todas as condições e exigências estabelecidas no Edital da licitação em referência e do Contrato a ser celebrado, cuja minuta constitui o Anexo "A" do Edital.

Declaramos, ainda, que inexistente qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista com servidor ou dirigente do Ministério dos Transportes.

<Local>, <dia> de <mês> de <ano>.

Responsável/Representante da Empresa

<Nome do Responsável>

Cargo



MINISTÉRIO DOS TRANSPORTES
SECRETARIA-EXECUTIVA
SUBSECRETARIA DE GESTÃO ESTRATÉGICA, TECNOLOGIA E INOVAÇÃO
COORDENAÇÃO-GERAL DE ENTREGA DE SERVIÇOS DE TECNOLOGIA
COORDENAÇÃO DE INFRAESTRUTURA TECNOLÓGICA

ANEXO - C

MODELO DE ORDEM DE SERVIÇO (OS)

INTRODUÇÃO			
<p>Por intermédio da Ordem de Serviço (OS) será solicitado formalmente à Contratada a prestação de serviço relativos ao objeto do contrato.</p> <p>O encaminhamento das demandas deverá ser planejado visando garantir que os prazos para entrega final de todos os serviços estejam compreendidos dentro do prazo de vigência contratual.</p> <p>Referência: Art. 32 IN SGD Nº 94/2022.</p>			
1 – IDENTIFICAÇÃO			
Nº da OS	<nº da OS>	Data de emissão	<dd/mm/aaaa>
CONTRATO/NOTA DE EMPENHO nº	<nº do contrato/nº da NE>		
Objeto do Contrato	<objeto do contrato>		
Contratada	<nome da contratada>	CNPJ	<nº do CNPJ>
Preposto	<nome do preposto>		
Início vigência	<dd/mm/aaaa>	Fim vigência	<dd/mm/aaaa>
ÁREA REQUISITANTE			
Unidade	<Sigla – Nome da unidade>		
Solicitante	<nome do solicitante>	E-mail	<endereço eletrônico>

2 – ESPECIFICAÇÃO DOS SERVIÇOS E VOLUMES ESTIMADOS					
Item	Descrição do serviço	Métrica	Valor unitário (R\$)	Qtde/Vol.	Valor Total (R\$)
1
...
Valor total estimado da OS					

3 – <INSTRUÇÕES/ESPECIFICAÇÕES> COMPLEMENTARES
<p><Incluir instruções complementares à execução da OS></p> <p><Ex.: Contatar a área solicitante para agendamento do horário de entrega></p> <p><Ex.: Conforme consta no Termo de Referência, o recebimento provisório está condicionado à entrega do código no ambiente de homologação, e a documentação do software no repositório oficial de gestão de projetos></p>

4 – DATAS E PRAZOS PREVISTOS			
Data de Início:	<dd/mm/aaaa>	Data do Fim:	<dd/mm/aaaa>
CRONOGRAMA DE EXECUÇÃO/ENTREGA			
Item	Tarefa/entrega	Início	Fim
1		<dd/mm/aaaa>	<dd/mm/aaaa>
2		<dd/mm/aaaa>	<dd/mm/aaaa>
3			

5 – ARTEFATOS / PRODUTOS	
Fornecidos	A serem gerados e/ou atualizados

6 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA

Autoriza-se a <execução dos serviços> correspondentes à presente [Ordem de Serviço](#), no período e nos quantitativos acima identificados.

(assinado eletronicamente)

<Nome>

**<Responsável pela demanda/Fiscal
Requisitante>**

(assinado eletronicamente)

<Nome>

Gestor do Contrato

<Local>, <dia> de <mês> de <ano>.



MINISTÉRIO DOS TRANSPORTES
SECRETARIA-EXECUTIVA
SUBSECRETARIA DE GESTÃO ESTRATÉGICA, TECNOLOGIA E INOVAÇÃO
COORDENAÇÃO-GERAL DE ENTREGA DE SERVIÇOS DE TECNOLOGIA
COORDENAÇÃO DE INFRAESTRUTURA TECNOLÓGICA

ANEXO - D

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO

O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da CONTRATADA em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da CONTRATANTE em decorrência de relação contratual, vigente ou não.

Referência: Art. 18, Inciso V, alínea “a” da IN SGD/ME Nº 94/2022.

Pelo presente instrumento o MINISTÉRIO DOS TRANSPORTES, <endereço>, doravante denominado **CONTRATANTE**, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ nº <Nº do CNPJ>, doravante denominada **CONTRATADA**;

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

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

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

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

1 – OBJETO

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

2 – CONCEITOS E DEFINIÇÕES

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

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

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

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

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições,

informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4 – DOS LIMITES DO SIGILO

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

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

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

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

5 – DIREITOS E OBRIGAÇÕES

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

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

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite

formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

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

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

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

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

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

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

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

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e

outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

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

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

6 – VIGÊNCIA

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

7 – PENALIDADES

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

8 – DISPOSIÇÕES GERAIS

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

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios

de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

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

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

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

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

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

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

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

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

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

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

9 – FORO

A CONTRATANTE elege o foro da Justiça Federal - Seção Judiciária do Distrito Federal, em Brasília-DF, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 – ASSINATURAS

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

CONTRATADA	CONTRATANTE
------------	-------------

<Nome>
<Qualificação>

<Nome>

TESTEMUNHAS

<Nome>
<Qualificação>

<Nome>
<Qualificação>

<Local>, <dia> de <mês> de <ano>.



MINISTÉRIO DOS TRANSPORTES
SECRETARIA-EXECUTIVA
SUBSECRETARIA DE GESTÃO ESTRATÉGICA, TECNOLOGIA E INOVAÇÃO
COORDENAÇÃO-GERAL DE ENTREGA DE SERVIÇOS DE TECNOLOGIA
COORDENAÇÃO DE INFRAESTRUTURA TECNOLÓGICA

ANEXO - E

TERMO DE CIÊNCIA

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

1 – IDENTIFICAÇÃO			
CONTRATO Nº	<nº do contrato>		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	CNPJ	<nº do CNPJ>
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	MATR.	<nº da Matrícula SIAPE>

2 – CIÊNCIA

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

Funcionários da CONTRATADA		
Nome	Matrícula	Assinatura
<Nome do(a) Funcionário(a)>	<nº da Matrícula>	
<Nome do(a) Funcionário(a)>	<nº da Matrícula>	
...

<Local>, <dia> de <mês> de <ano>.