

INST.FED.DE EDUC.,CIENC. E TECNOLOGIA PIAUÍ

Termo de Referência 127/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
127/2026	158146-INST.FED.DE EDUC.,CIENC. E TECNOLOGIA PIAUÍ	ANTONIO FRANCISCO MARTINS FORTES	18/09/2026 09:53 (v 0.8)
Status	ASSINADO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC	153/2026	23172.000426/2026-34

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

Ministério da Educação

Instituto Federal de Educação, Ciência e Tecnologia do Piauí

Av. Jânio Quadros, 330, Santa Isabel, TERESINA / PI,CEP 64053-390

Fone: (86) 3131-1443 Site: www.ifpi.edu.br

TERMO DE REFERÊNCIA

Pregão Eletrônico nº 00153/2026

(Processo Administrativo nº 23172.000426/2026-34)

1.1. Contratação de licenças de uso de software de antivírus corporativo, com a atualização contínua por 36 meses, para servidores, estações Linux e Windows, para anteder demandas do IFPI, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

1.1.1. Contratação de solução corporativa de antivírus, compreendendo licenciamento/subscrição, atualização contínua e suporte técnico associado por 36 meses.

1.1.2. A presente contratação constitui uma única Solução de Tecnologia da Informação e Comunicação – TIC, nos termos do art. 3º, inciso I, da IN SGD/ME nº 94/2022, considerando a integração funcional e operacional entre os componentes de licenciamento, atualização, gerenciamento centralizado, proteção de endpoints e suporte técnico especializado.

Item	Especificação	CATSER			Quantidade	Valor Unitário	Valor Total
------	---------------	--------	--	--	------------	----------------	-------------

			Métrica ou Unidade de Medida	CÓD. PMC-TIC			
1	Contratação de licenças de uso de antivírus corporativo, com atualização contínua por 36 meses, para servidores, estações Linux e Windows.	27502	Un.		3000	R\$ 190,26	R\$ 570.780,00
					TOTAL GLOBAL		R\$ 570.780,00

Classificação do objeto quanto à heterogeneidade ou complexidade

1.2. O(s) serviço(s) objeto desta contratação são caracterizados como **comum(ns)**, conforme justificativa constante do Estudo Técnico Preliminar.

Classificação do objeto quanto ao modelo de execução

1.3. O serviço é enquadrado como continuado tendo em vista que é essencial para a manutenção da atividade administrativa, sendo a vigência plurianual mais vantajosa considerando os custos da contratação;

Prazo de vigência

1.4. O prazo de vigência da contratação é de **36 meses** contados da **emissão da Nota de Empenho**, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021

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

1.6. O prazo de vigência da Ata de Registro de preços será de 12 (doze) meses e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso, na forma do artigo 84 da Lei nº 14.133, de 2021.

1.6.1. A adoção do Sistema de Registro de Preços é justificada com base no art. 3º, II, do Decreto nº 11.462 /2023 que menciona o cabimento de registro de preços quando for conveniente a aquisição de bens com previsão de entregas parceladas. Dessa forma, considerando a quantidade e tipos de itens que compõem a aquisição, entende-se haver compatibilidade com as hipóteses previstas no Decreto nº 11.462/2023.

1.6.2. A presente contratação será realizada mediante Sistema de Registro de Preços, sendo admitida a participação de órgãos e entidades da Administração Pública na condição de participantes, desde que previamente integrados aos procedimentos iniciais de planejamento da contratação e da Intenção de Registro de Preços – IRP, observadas as disposições da Lei nº 14.133/2021 e regulamentação aplicável.

1.7. O fornecimento de bens não contempla item de Catálogo de produtos com Condições Padronizadas publicados pelo Órgão Central do SISP, previsto na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

1.8. O IFPI ainda não possui o Plano Diretor de Logística Sustentável, o qual deverá ser implementado em oportunidade futura.

1.9. Não será permitida adesão à Ata de Registro de Preços decorrente desta contratação por órgãos ou entidades não participantes.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A presente contratação justifica-se fornecimento de 3.000 (três mil) licenças de solução corporativa de antivírus, com atualização contínua, suporte técnico e gerenciamento centralizado, destinadas à proteção dos ativos computacionais do Instituto Federal de Educação, Ciência e Tecnologia do Piauí – IFPI, abrangendo estações de trabalho, notebooks e servidores utilizados nas atividades administrativas e acadêmicas da instituição.

2.2. A contratação justifica-se pela necessidade contínua de proteção dos ambientes computacionais do IFPI contra ameaças cibernéticas, tais como vírus, malwares, ransomwares, spywares, ataques de exploração de vulnerabilidades, códigos maliciosos e demais ameaças digitais que possam comprometer a confidencialidade, integridade e disponibilidade das informações institucionais.

2.3. Considerando o crescente volume de acessos à internet, utilização de serviços em nuvem, compartilhamento de arquivos, uso de correio eletrônico institucional e integração entre sistemas corporativos, faz-se imprescindível a manutenção de solução especializada de segurança digital capaz de prover mecanismos avançados de prevenção, detecção, bloqueio, quarentena e remediação de ameaças em tempo real.

2.4. A ausência de solução corporativa de antivírus ou eventual descontinuidade do serviço poderá ocasionar sérios impactos operacionais e administrativos ao IFPI, incluindo:

- indisponibilidade de serviços institucionais;
- comprometimento de sistemas acadêmicos e administrativos;
- vazamento ou perda de dados institucionais;
- interrupção de atividades pedagógicas e administrativas;
- propagação de códigos maliciosos na rede corporativa;
- prejuízos financeiros e operacionais decorrentes de incidentes de segurança da informação;
- descumprimento de diretrizes legais e normativas relacionadas à segurança da informação e proteção de dados.

2.5. A contratação encontra-se alinhada às boas práticas de Segurança da Informação e Comunicação, bem como aos princípios estabelecidos pela Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), especialmente no que se refere à adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais tratados pela instituição.

2.6. Ressalta-se que o IFPI já utiliza solução corporativa de antivírus baseada na plataforma Kaspersky Endpoint Security for Business Select, atualmente implantada e operacional em sua infraestrutura tecnológica. Nesse contexto, a presente contratação visa assegurar a continuidade da solução já utilizada institucionalmente, preservando a padronização tecnológica adotada pela equipe de Tecnologia da Informação do IFPI.

2.7. A manutenção da solução atualmente implantada apresenta vantagens técnicas e operacionais relevantes, dentre as quais destacam-se:

- 2.7.1. preservação da compatibilidade técnica com os ambientes Windows e Linux já existentes;
- 2.7.2. continuidade da utilização da console centralizada de gerenciamento;
- 2.7.3. manutenção das políticas de segurança já implementadas;
- 2.7.4. redução de riscos operacionais decorrentes de processos de migração;
- 2.7.5. eliminação da necessidade de reimplantação completa da solução;
- 2.7.6. aproveitamento do conhecimento técnico já adquirido pela equipe de TI;
- 2.7.7. redução de custos indiretos com treinamento, adaptação e suporte especializado;
- 2.7.8. continuidade dos mecanismos já consolidados de monitoramento e resposta a incidentes.

2.8. Além disso, a solução atualmente utilizada atende satisfatoriamente às necessidades institucionais do IFPI, especialmente quanto:

- 2.8.1. ao gerenciamento centralizado dos endpoints;
- 2.8.2. à proteção de estações de trabalho e servidores;
- 2.8.3. à atualização contínua das assinaturas de segurança;
- 2.8.4. à proteção contra ameaças conhecidas e desconhecidas;
- 2.8.5. à compatibilidade com diferentes sistemas operacionais;
- 2.8.6. à implementação de políticas corporativas de segurança;
- 2.8.7. ao controle e monitoramento dos dispositivos protegidos.

2.9. Sob o aspecto da economicidade e eficiência administrativa, a continuidade da utilização da solução já implantada mostra-se mais vantajosa para a Administração Pública, tendo em vista que evita custos adicionais relacionados à substituição tecnológica, reconfiguração do ambiente computacional, treinamentos, migração de políticas de segurança e possíveis indisponibilidades operacionais decorrentes da troca de fabricante.

2.10. A contratação também encontra respaldo nos princípios da continuidade do serviço público, eficiência administrativa e mitigação de riscos à segurança da informação, sendo considerada essencial para manutenção das atividades institucionais do IFPI.

2.11. Adicionalmente, a presente demanda encontra aderência às diretrizes previstas:

- 2.11.1. na Lei nº 14.133/2021;
- 2.11.2. na Instrução Normativa SGD/ME nº 94/2022;
- 2.11.3. na Política de Segurança da Informação da Administração Pública Federal;
- 2.11.4. na Lei Geral de Proteção de Dados Pessoais – LGPD;

2.11.5. nas boas práticas de governança e segurança cibernética aplicáveis à Administração Pública Federal. 2.12. Dessa forma, conclui-se que a contratação pretendida é necessária, adequada e indispensável para assegurar a continuidade da proteção dos ativos computacionais do IFPI, garantindo maior segurança, disponibilidade e confiabilidade aos serviços institucionais suportados pela infraestrutura de tecnologia da informação da instituição.

2.12. Dessa forma, conclui-se que a contratação pretendida é necessária, adequada e indispensável para assegurar a continuidade da proteção dos ativos computacionais do IFPI, garantindo maior segurança, disponibilidade e confiabilidade aos serviços institucionais suportados pela infraestrutura de tecnologia da informação da instituição

2.13. O objeto da contratação está previsto no Plano de Contratações Anual 2025, conforme consta das informações básicas deste termo de referência.

2.14. O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2024-2027 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2022-2024 do IFPI, que teve sua vigência prorrogada, pela resolução normativa CONSUP/OSUPCOL/REI /IFPI N° 236 até 31/12/2025 conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos
	Entregar e manter soluções de Tecnologia da Informação alinhadas à estratégia do IFPI. Desenvolver, implantar e manter soluções de Tecnologia da Informação que atendam às

OE01	diretrizes e projetos estratégicos do IFPI e outras demandas que tenham sido priorizadas pelo Instituto.
OE09	Pesquisar e conhecer as tecnologias emergentes com o objetivo de avaliar os benefícios de sua adoção no IFPI.
OE10	Promover mudanças na infraestrutura tecnológica que resultem em condições adequadas para a realização das atividades do IFPI, envolvendo melhorias das ferramentas de trabalho e equipamentos

ALINHAMENTO AO PDTIC 2026			
ID	Ação do PDTIC	ID	Meta do PDTIC associada
AC. 02. Capl. 01	Fortalecer a infraestrutura de Tecnologia da Informação(bens e serviços)	N1. 12.	Atualização ou aquisição de software (Sistema de monitoramento e gerência de máquinas dos laboratórios de informática, Softwares de suporte ao DATACENTER Institucional, Softwares para programação visual, Softwares para a produção audiovisual, aquisição de licenças para S.O, suíte de escritório e softwares para uso acadêmico e administrativo)

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

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

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 em Contratação de licenças de uso de antivírus corporativo com monitoramento em tempo real e proteção de vulnerabilidades para servidores, estações Linux e Windows, pelo período de 36 meses conforme especificações gerais abaixo:

3.2.1. Todos os componentes que fazem parte da solução, de segurança para servidores e estações de trabalho, deverão ser fornecidos por um único fabricante.

3.2.2. Não serão aceitas composições de produtos de fabricantes diferentes.

3.2.3. O conjunto de softwares que compõe a solução de antivírus para servidores e estações de trabalho deverão ser totalmente gerenciáveis através da mesma console de gerenciamento centralizado e de forma que todos os produtos sejam monitorados através desta.

3.2.4. A solução deverá possuir ferramentas de varredura, detecção, análise e remoção de malwares, riskwares, spywares e demais formas de vírus e códigos maliciosos conhecidos, bem como firewall, ids/ips, controle de aplicativos, controle de conexão, atualizador de softwares, controle de conteúdo web e quarentena de rede.

3.2.5. A solução deverá também possuir ferramentas de análise e remoção de ameaças desconhecidas, monitorando o seu comportamento e bloqueando potenciais ameaças em tempo real.

3.2.6 Estas devem ser totalmente integradas, instaladas através de um único pacote sem a necessidade de instalação de módulos.

3.3. Características Gerais

1. **Do módulo de proteção de endpoint**

1. A solução proposta deverá proteger os sistemas operacionais abaixo:

1. Windows 7
2. Windows 8
3. Windows 8.1
4. Windows 10
5. Windows 11

2. Servidores

1. Windows Small Business Server 2011
2. Windows MultiPoint Server 2011
3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

3. Servidores de terminal Microsoft

1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

4. Sistemas operacionais Linux de 32 bits:

1. CentOS 6.7 e posterior
2. Debian GNU/Linux 11.0 e posterior
3. Debian GNU/Linux 12.0 e posterior
4. Red Hat Enterprise Linux 6.7 e posterior

5. Sistemas operacionais Linux de 64 bits:

1. Amazon Linux 2.
2. CentOS 6.7 e mais tarde
3. CentOS 7.2 e posterior.
4. CentOS Stream 8.
5. CentOS Stream 9.
6. Debian GNU/Linux 11.0 e posterior.
7. Debian GNU/Linux 12.0 e posterior.
8. Linux Mint 20.3 e superior.
9. Linux Mint 21.1 e posterior.
10. openSUSE Leap 15.0 e posterior.
11. Oracle Linux 7.3 e posterior.
12. Oracle Linux 8.0 e posterior.
13. Oracle Linux 9.0 e posterior.
14. Red Hat Enterprise Linux 6.7 e posterior
15. Red Hat Enterprise Linux 7.2 e posterior.
16. Red Hat Enterprise Linux 8.0 e posterior.
17. Red Hat Enterprise Linux 9.0 e posterior.
18. Rocky Linux 8.5 e posterior. Rocky Linux 9.1.
19. SUSE Linux Enterprise Server 12.5 ou posterior.
20. SUSE Linux Enterprise Server 15 ou posterior.
21. Ubuntu 20.04 LTS.
22. Ubuntu 22.04 LTS.
23. Sistemas operacionais Arm de 64 bits.
24. CentOS Stream 9.
25. SUSE Linux Enterprise Server 15.
26. Ubuntu 22.04 LTS.

6. Sistemas operacionais MAC OS:

1. macOS 12 – 14

7. Ferramentas de virtualização MAC OS:

1. Parallels Desktop 16 para Mac Business Edition
2. VMware Fusion 11.5 Professional

3. *VMware Fusion 12 Profissional*
8. *A solução proposta deverá suportar as seguintes plataformas virtuais:*
 1. *VMware Workstation 17.0.2 Pro*
 2. *VMware ESXi 8.0 Update 2*
 3. *Microsoft Hyper-V Server 2019*
 4. *Citrix Virtual Apps e Desktop 7 2308*
 5. *Citrix Provisioning 2308*
 6. *Citrix Hypervisor 8.2 Update 1*

2. Do módulo de gerenciamento avançado

1. *A solução proposta deve suportar arquitetura cloud-native e on-premise;*
2. *A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:*
 1. *Amazon Web Services*
 2. *Microsoft Azure*
3. *A solução proposta deve incluir as seguintes opções de integração SIEM:*
 1. *HP (Microfoco) ArcSight*
 2. *IBM QRadar*
 3. *Splunk*
 4. *Kaspersky KUMA*
4. *A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.*
5. *A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança prédefinidas;*
6. *A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.*
7. *O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.*
8. *A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.*
9. *A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.*
10. *A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.*
11. *A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.*
12. *A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.*
13. *O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem*
14. *O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em um único/múltiplos dispositivos com base nas seguintes regras de ativação:*
 1. *Status do dispositivo*
 2. *Tag*
 3. *Diretório ativo*
 4. *Proprietários de dispositivos*
 5. *Hardware*
15. *A solução proposta deve suportar os seguintes canais de entrega de notificação:*
 1. *E-mail*
 2. *Registro de sistema*
 3. *SMS*
16. *A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:*
 1. *Atributos de rede*
 2. *Nome*
 3. *Domínio e/ou Sufixo de Domínio*

4. *Endereço de IP*
5. *Endereço IP para servidor de gerenciamento*
6. *Localização no Active Directory*
7. *Unidade organizacional*
8. *Grupo*
9. *Sistema operacional*
10. *Número do pacote de serviço*
11. *Arquitetura Virtual*
12. *Registro de aplicativos*
13. *Nome da Aplicação*
14. *Versão do aplicativo*
15. *Fabricante*
16. *Tipo e versão*
17. *Arquitetura*
17. *A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.*
18. *A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública*
19. *As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:*
 1. *Dispositivos Desktop/Servidores*
 2. *Dispositivos móveis*
 3. *Dispositivos de rede*
 4. *Dispositivos virtuais*
 5. *Componentes OEM*
 6. *Periféricos de computador*
 7. *Dispositivos IoT conectados*
 8. *Telefones VoIP*
 9. *Repositórios de rede*
20. *A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:*
 1. *Nome da Aplicação*
 2. *Caminho do aplicativo*
 3. *Metadados do aplicativo*
 4. *Aplicativo Certificado digital*
 5. *Categorias de aplicativos predefinidas pelo fornecedor*
 6. *SHA256 e MD5*
21. *A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:*
 1. *Bluetooth*
 2. *Dispositivos móveis*
 3. *Modems externos*
 4. *CD/DVD*
 5. *Câmeras e scanners*
 6. *MTPs*
 7. *E a transferência de dados para dispositivos móveis*
22. *A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.*
23. *A solução sugerida deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.*
24. *A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:*
 1. *Estruturas de domínios e grupos de trabalho do Windows*
 2. *Estruturas de grupos do Active Directory*
 3. *Conteúdo de um arquivo de texto criado manualmente pelo administrador*

25. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.
26. A solução proposta deve permitir realizar as seguintes ações para endpoints:
 1. Verificação manual;
 2. Verificação no acesso;
 3. Verificação por demanda;
 4. Verificação de arquivos compactados
 5. Verificação de arquivos individuais, pastas e unidades;
 6. Bloqueio e verificação de scripts Proteção contra alteração de registros;
 7. Proteção contra estouro de buffer;
 8. Verificação em segundo plano/inativa
27. Verificação de unidade removível na conexão com o sistema;
28. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
29. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política /tarefa possam ser revisadas.
30. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
31. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
32. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
33. A solução proposta deve suportar Windows Failover Cluster.
34. A solução proposta deve ter um recurso de clustering integrado.
35. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
36. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
37. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
38. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo
39. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
40. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
41. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
42. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-ToLive (TTL) de pacotes.
43. A solução proposta deverá possuir controles para download de DLL e drivers.
44. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo específico de prevenção de intrusão.
45. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
46. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
47. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.

48. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
49. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
50. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
51. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
52. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança antimalware através do servidor de administração.
53. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
54. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações antimalware instalados, e para distribuir notificações sobre eventos por email.
55. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
56. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
57. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .
58. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
59. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.
60. A solução proposta deve permitir ao administrador personalizar relatórios.
61. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
62. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
63. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
64. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
65. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.
66. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.
67. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado /existente para esses dispositivos;
68. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

69. A solução proposta deve permitir instalar o módulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
1. Windows
 2. Linux
3. A solução proposta deverá suportar os seguintes servidores de banco de dados:
1. Windows:
 1. Microsoft SQL Server
 2. Microsoft Banco de dados SQL do Azure
 3. MySQL Standard e Enterprise
 4. MariaDB
 5. PostgreSQL
 2. Linux:
 1. MySQL
 2. MariaDB
 3. PostgreSQL
4. A solução proposta deverá suportar as seguintes plataformas virtuais:
1. Windows:
 1. VMware vSphere 6.7 e 7.0
 2. Estação de trabalho VMware 16 Pro
 3. Servidor Microsoft Hyper-V 2012 de 64 bits
 4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
 5. Microsoft Servidor Hyper -V 2016 de 64 bits
 6. Servidor Microsoft Hyper-V 2019 de 64 bits
 7. Servidor Microsoft Hyper-V 2022 de 64 bits
 8. Citrix XenServer 7.1 LTSR
 9. Citrix XenServer 8.x
 10. Oracle VM VirtualBox 6.x
 2. Linux:
 1. VMware vSphere 6.7, 7.0 e 8.0
 2. VMware Desktop 16 Pro e 17 Pro
 3. Servidor Microsoft Hyper-V 2012 de 64 bits
 4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
 5. Microsoft Servidor Hyper -V 2016 de 64 bits
 6. Servidor Microsoft Hyper-V 2019 de 64 bits
 7. Servidor Microsoft Hyper-V 2022 de 64 bits
 8. Citrix XenServer 7.1 e 8.x
 9. Oracle VM VirtualBox 6.x e 7.x
5. **Do módulo de gerenciamento simplificado**
1. A solução proposta deve suportar arquitetura cloud;
 2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.
 3. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.
 4. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.
 5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.
 6. A solução proposta deve atender as condições apontadas no item e subítemos 6. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.
 7. A solução proposta deve incluir informações do endpoint:
 1. IP público de internet;
 2. IP interno do dispositivo;
 3. Versão do agente de proteção;
 4. Última comunicação com a console, contendo data e hora;
 5. Informações do sistema operacional;

6. Requisitos gerais

1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
 1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
2. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).
4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
5. A solução proposta deve suportar o subsistema Linux no Windows.
6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
 1. Proteção contra ameaças sem arquivos (Fileless);
 2. Fornecimento de proteção baseada em machine learning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
7. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
8. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
9. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
10. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
11. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
12. A solução proposta deve fornecer análise comportamental baseada em machine learning.
13. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
14. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
 1. Controles de aplicativos,
 2. Controle web e dispositivos
 3. HIPS e Firewall
 4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
15. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
16. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
17. A solução proposta deve ter bancos de dados de reputação locais e globais.
18. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
19. A solução proposta deve incluir um módulo capaz, no mínimo, de:
 1. Bloqueio de aplicativos com base em sua categorização.
 2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
 3. A adição de sub-redes e a modificação de permissões de atividade.
20. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
21. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
22. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.
23. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
24. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

25. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.
26. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.
27. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.
28. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
29. A solução proposta deve ser capaz de decryptografar e verificar o tráfego de rede transmitido por conexões criptografadas.
30. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
31. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
32. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.
33. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
34. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.
35. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
36. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.
37. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
38. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
39. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
40. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
41. A solução proposta deve ter categoria de detecção para bloquear banners de sites.
42. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
43. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
44. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
45. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
46. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;
47. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
48. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
49. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.

50. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
51. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
52. A solução proposta deve suportar o controle de scripts executados em PowerShell.
53. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
54. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
55. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.
56. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
57. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
58. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
59. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
 1. Filtro de anexos.
 2. Verificação de mensagens de email ao receber, ler e enviar.
60. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
61. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
62. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
63. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registro do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
64. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
65. A solução proposta deve incluir suporte ao protocolo IPv6.
66. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
67. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
68. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.
69. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
70. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
71. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
72. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
73. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
74. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
75. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.
76. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.

77. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia, bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
78. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
79. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
80. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
81. A solução proposta deve suportar endereços IPv6.
82. A solução proposta deve suportar verificação em duas etapas (autenticação)
83. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
84. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
85. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.
86. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
87. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
88. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
89. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
90. A solução proposta deve permitir a gestão de um componente que controle o trabalho com dispositivos de E/S externos.
91. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
92. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.
93. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
94. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
95. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
96. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.
97. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
98. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
99. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
100. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
101. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.
102. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.
103. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
104. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

105. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.
106. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
107. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
 1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
 2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
108. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.
109. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

7. Do modulo de gerenciamento de dispositivos móveis

1. O modulo deve ser integrado a console de gerenciamento;
2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
 1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)
3. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
 1. iOS 10–17 ou iPadOS 13–17
4. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
5. A solução proposta deve suportar dispositivos iOS supervisionados.
6. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.
7. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.
8. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.
9. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).
10. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.
11. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.
12. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.
13. A solução proposta deve ter recursos de containerização para dispositivos Android.
14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
 1. Dados em contêineres
 2. Contas de e-mail corporativo
 3. Configurações para conexão à rede Wi-Fi corporativa e VPN
 4. Nome do ponto de acesso (APN)
 5. Perfil do Android for Work
 6. Recipiente KNOX
 7. Chave do gerenciador de licença KNOX
15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
 1. Todos os perfis de configuração instalados
 2. Todos os perfis de provisionamento
 3. O perfil iOS MDM
16. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

17. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo.
18. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controle de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:
 1. Critérios de verificação do dispositivo;
 2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
19. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.
20. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
 1. Cartões de memória e outras unidades removíveis
 2. Câmera do dispositivo
 3. Conexões Wi-Fi
 4. Conexões Bluetooth
 5. Porta de conexão infravermelha
 6. Ativação do ponto de acesso Wi-Fi
 7. Conexão de área de trabalho remota
 8. Sincronização de área de trabalho
 9. Definir configurações da caixa de correio do Exchange
 10. Configurar caixa de e-mail em dispositivos iOS MDM
 11. Configure contêineres Samsung KNOX.
 12. Definir as configurações do perfil do Android for Work
 13. Configurar e-mail/calendário/contatos
 14. Defina as configurações de restrição de conteúdo de mídia.
 15. Definir configurações de proxy no dispositivo móvel
 16. Configurar certificados e SCEP
21. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay.
22. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel: G
 1. oogle Play, Huawei App Gallery e Apple App Store
 2. Portal de inscrição móvel KNOX
 3. Pacotes de instalação pré-configurados independentes
23. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.
24. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
25. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
 1. VMware AirWatch 9.3 ou posterior
 2. MobileIron 10.0 ou posterior
 3. IBM MaaS360 10.68 ou posterior
 4. Microsoft Intune 1908 ou posterior
 5. SOTI MobiControl 14.1.4 (1693) ou posterior
26. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
27. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
 1. Google Play
 2. Galeria de aplicativos Huawei
 3. Loja de aplicativos da Apple
28. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
29. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.
30. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.

31. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
32. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
33. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
34. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
35. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
36. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
37. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
38. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
39. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido /Permitido.
40. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
41. A solução proposta deve proteger contra ameaças online em dispositivos iOS

8. **Do módulo de EDR**

1. Deve apresentar um gráfico de propagação de ameaças com os principais processos, conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
4. Deve apresentar as seguintes informações:
 1. Processo;
 2. Arquivos;
 3. Chaves de registros;
 4. Conexões de rede;
 5. SHA256 e MD5;
5. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
6. Deve apresentar informações detalhadas contendo:
 1. Usuário que executou a ação;
 2. Informações acesso privilegiado;

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio:

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

4.1.1. Proteção de dados independentemente de onde estão armazenados seja em ambientes locais ou compartilhamentos entre os dispositivos do IFPI.

4.1.2. Inspeção do tráfego web, possibilitando validar acessos a conteúdos suspeitos ou maliciosos.

4.1.3. À medida que as estações de trabalho são distribuídas em diferentes locais, sejam ambientes internos ou home office, a capacidade de impor consistentemente as políticas de segurança e conformidade se torna ainda mais crítica;

4.1.4. Possibilidade de otimização de todas as operações de gerenciamento de sistemas e endpoints obtendo economias imediatas e eficiências organizacionais. A partir do conceito do portfólio unificado de segurança e gerenciamento de endpoints padronizado em toda a infraestrutura de TI;

4.1.5. Capacidade de entregar serviço avançado e redução de problemas na instalação, através da implementação de sistemas e processos de migração padronizados;

4.1.6. Possibilidade de monitoração e o fortalecimento contínuos da segurança para servidores locais; Capacidade de implementar automaticamente o Anti-Malware e a proteção contra ameaças na rede ambientes Windows;

4.1.7. Capacidade de fornecer informações de segurança prontas, através de políticas, habilitando serviços de proteção centrados no aplicativo e integrados ao Windows;

4.1.8. Possibilidade de implementar ações de quarentena de arquivos nos servidores protegidos com aplicação baseada em política;

4.1.9. Capacidade de integração e monitoração com a grande maioria das plataformas de monitoramento, proporcionando controle das informações.

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, de 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 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

Requisitos de Manutenção

4.4. Devido às características da solução, há necessidade de realização de manutenções **corretivas/preventivas /adaptativa/evolutiva** pela Contratada, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades;

4.4.1. Conforme recomendado, a solução escolhida encontra-se estabelecida no ambiente tecnológico do instituto, dispensa a contratação de implantação e despesas com cursos de treinamento.

Requisitos Temporais

4.5. Os serviços devem ser prestados no prazo máximo de **30** dias corridos para as capitais dos estados e de **60** dias corridos para as demais localidades, a contar do recebimento da abertura da Ordem de Serviço (OS), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

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

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

4.8. Na execução dos serviços, deverão ser observados os seguintes prazos:

4.8.1. Constatada a ocorrência de divergência na especificação do produto entregue, fica a CONTRATADA obrigada a providenciar a substituição em até 15 (quinze) dias corridos, contados a partir do recebimento da notificação da ocorrência por parte da CONTRATANTE.

4.8.2. As licenças serão recebidas provisoriamente no prazo de 05 (cinco) dias úteis, pelo (a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

4.8.3. As Licenças poderão ser rejeitadas, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 05 (cinco) dias úteis, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

4.8.4. As Licenças serão recebidas definitivamente no prazo de 10 (dez) dias corridos, contados do recebimento provisório, após a verificação da qualidade e consequente aceitação mediante termo circunstanciado.

4.9. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

Requisitos de Segurança e Privacidade

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

4.10.1. A CONTRATADA se obriga a tratar como informações sigilosas e privadas do IFPI quaisquer dados e informações relacionados à prestação dos serviços, utilizando-as apenas para as finalidades previstas no Contrato, não podendo revelá-las ou facilitar informações a terceiros;

4.10.2. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE;

4.10.3. Caso haja necessidade de substituição de dispositivos de armazenamento de dados, a CONTRATADA se obriga a prover forma efetiva e segura de eliminação dos dados presentes nos HDs/SSDs recolhidos, de forma a manter o sigilo dos dados em alinhamento à Política de Segurança da Informação do IFPI e da Lei Geral de Proteção de Dados;

4.10.4. A CONTRATADA se obriga a observar a Lei Geral de Proteção de Dados;

4.10.5. A CONTRATADA se responsabilizará pelo ressarcimento por prejuízos causados pela inobservância dos itens acima ou outros de qualquer natureza, inclusive danos a terceiros;

4.10.6. Para demais situações de segurança não previstas neste Termo, a CONTRATADA se submeterá às políticas de segurança da informação e comunicação internas da CONTRATANTE;

Requisitos Sociais, Ambientais e Culturais

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

4.11.1. Os profissionais do Contratado, quando presentes nas instalações da Contratante, deverão apresentar-se vestidos de forma adequada ao ambiente de prestação dos serviços (trabalho), evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da ANP ou que ofenda o senso comum de moral e bons costumes.

4.11.2. Os profissionais do Contratado deverão respeitar todos os servidores, funcionários e colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo.

4.11.3. A prestação de serviços objeto deste Termo de Referência não gera vínculo empregatício entre os empregados do Contratado e a Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação.

4.11.4. A documentação das atividades e documentos produzidos pelo Contratado deverá estar em língua portuguesa de forma clara, objetiva e gramaticalmente correta.

Requisitos da Arquitetura Tecnológica

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

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

4.13.1. A CONTRATADA deverá prover softwares atualizados com as últimas versões disponibilizadas pelo fabricante;

4.13.2. A CONTRATADA deverá prover instalador da solução contratada, assim como, suas atualizações;

Requisitos de Projeto e de Implementação

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

4.14.1. Não se aplica pela natureza do objeto.

Requisitos de Implantação[A10]

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

4.15.1. A CONTRATADA deverá prover softwares atualizados com as últimas versões disponibilizadas pelo fabricante;

4.15.2. A CONTRATADA deverá prover instalador da solução contratada, assim como, suas atualizações;

Requisitos de Garantia e Manutenção

4.16. *O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo, 36 meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.*

4.17. A CONTRATADA assegurará, durante o período de garantia, o perfeito e integral funcionamento do software, sem ônus para a CONTRATANTE;

4.18. Durante todo o período de garantia deverá ser disponibilizado para a instalação em até 15 dias de seu lançamento, todas as atualizações de produto, assim como, novas versões;

4.19. Suporte na modalidade 8x5x365 deverá ser realizado pela CONTRATADA;

4.20. Durante o período de garantia do software, a CONTRATADA deverá prestar, sem ônus adicional para a CONTRATANTE, na localidade onde os softwares estiverem instalados, assistência técnica oferecendo, no mínimo, os seguintes serviços:

4.21. Atendimento telefônico, com funcionamento de segunda a sexta-feira, das 08:00 às 17:00 horas, para registro e acompanhamento dos chamados de suporte técnico visando esclarecer dúvidas relativas ao uso dos componentes da solução;

Requisitos de Experiência Profissional

4.22. *Não serão exigidos requisitos de experiência profissional para a presente contratação.*

Requisitos de Formação da Equipe

4.23. *Os serviços deverão ser prestados por técnicos devidamente capacitados, de acordo com os critérios estabelecidos a seguir:*

4.23.1. Considerando que a solução corporativa de antivírus já se encontra implantada e operacional no ambiente tecnológico do Instituto Federal de Educação, Ciência e Tecnologia do Piauí – IFPI, a equipe técnica da

CONTRATADA deverá possuir qualificação compatível com atividades de suporte técnico, sustentação, manutenção, atualização e atendimento especializado da solução contratada.

4.23.2. Os profissionais disponibilizados pela CONTRATADA deverão possuir conhecimentos técnicos relacionados à administração e suporte de soluções corporativas de proteção de endpoints, incluindo:

- gerenciamento centralizado de antivírus corporativo;
- análise e tratamento de incidentes de segurança;
- atualização e manutenção de agentes de proteção;
- troubleshooting em estações de trabalho e servidores;
- gerenciamento de políticas de segurança;
- monitoramento de eventos e alertas;
- suporte a ambientes Windows e Linux;
- suporte a consoles centralizadas de gerenciamento.

4.23.3. A CONTRATADA deverá manter, durante toda a vigência contratual, equipe técnica apta a prestar suporte especializado à solução utilizada pelo IFPI, especialmente no atendimento de incidentes relacionados:

- à detecção de ameaças;
- a falhas de atualização;
- à comunicação entre endpoints e console de gerenciamento;
- à aplicação de políticas de segurança;
- à indisponibilidade de agentes;
- a problemas de desempenho relacionados à solução de proteção;
- a eventos de segurança identificados nos ativos institucionais.

4.23.4. Os profissionais responsáveis pelo suporte técnico deverão possuir experiência comprovada em atendimento e sustentação de soluções corporativas de antivírus, preferencialmente da plataforma Kaspersky Endpoint Security for Business Select ou equivalente.

4.23.5. A comprovação da qualificação técnica poderá ser realizada mediante:

- certificados oficiais emitidos pelo fabricante;
- certificados de treinamento;
- declarações técnicas;
- atestados de capacidade técnica da empresa;
- documentação comprobatória de experiência profissional compatível com o objeto da contratação.

4.23.6. A CONTRATADA deverá disponibilizar profissionais capacitados para atendimento remoto e, quando necessário, presencial, visando apoiar a equipe técnica do IFPI na resolução de incidentes, falhas operacionais e demais ocorrências relacionadas à solução contratada.

4.23.7. Considerando que a solução já se encontra implantada e em uso institucional, não será exigida experiência específica relacionada à implantação inicial da ferramenta, migração de ambientes ou execução de projetos de implantação, mas sim experiência em:

- suporte técnico especializado;
- manutenção operacional;
- atualização da solução;
- atendimento de chamados;
- sustentação de ambiente corporativo protegido.

4.23.8. A exigência de equipe técnica qualificada visa garantir:

- continuidade da proteção dos ativos computacionais do IFPI;
- redução do tempo de resposta em incidentes;
- estabilidade operacional da solução;
- adequada execução dos serviços de suporte técnico;
- manutenção da segurança da informação institucional.

4.23.9. A equipe técnica da CONTRATADA deverá manter-se atualizada em relação às versões, funcionalidades, atualizações corretivas e evolutivas disponibilizadas pelo fabricante durante toda a vigência contratual.

4.23.10. A CONTRATADA deverá assegurar que os profissionais envolvidos na execução contratual observem as normas de segurança da informação, sigilo e confidencialidade aplicáveis ao ambiente institucional do IFPI.

Requisitos de Metodologia de Trabalho

4.24. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.

4.25. A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.

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

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

Requisitos de Segurança da Informação e Privacidade

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

4.28.1. A CONTRATADA deverá observar integralmente as normas, políticas, padrões e procedimentos de Segurança da Informação e Comunicação adotados pelo Instituto Federal de Educação, Ciência e Tecnologia do Piauí – IFPI, bem como a legislação aplicável à Administração Pública Federal.

4.28.2. A execução contratual deverá observar os princípios e diretrizes estabelecidos:

4.28.2.1. na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

4.28.2.2. na Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI);

4.28.2.3. na Lei nº 14.133/2021;

4.28.2.4. na Instrução Normativa SGD/ME nº 94/2022;

4.28.2.5. nas políticas institucionais de Segurança da Informação do IFPI;

4.28.2.6. nas boas práticas aplicáveis à segurança cibernética e proteção de dados.

4.28.3. A CONTRATADA deverá garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações, dados e ativos computacionais eventualmente acessados em razão da execução contratual.

4.28.4. A CONTRATADA e seus profissionais deverão tratar como sigilosas todas as informações institucionais às quais tenham acesso, sendo vedada:

4.28.4.1. a divulgação; a reprodução; o compartilhamento; a utilização indevida; a retenção não autorizada de dados ou informações pertencentes ao IFPI.

4.28.5. Os profissionais envolvidos na execução contratual deverão manter sigilo absoluto sobre quaisquer dados, informações, credenciais, configurações, registros de eventos, topologias de rede ou informações técnicas do ambiente computacional do IFPI, mesmo após o encerramento do contrato.

4.28.6. A CONTRATADA deverá adotar controles adequados de segurança para impedir acessos não autorizados, vazamentos de informações, perda de dados ou qualquer incidente que comprometa a segurança dos ambientes protegidos.

4.28.7. Sempre que houver necessidade de acesso remoto aos ambientes do IFPI, a CONTRATADA deverá utilizar mecanismos seguros de autenticação, rastreabilidade e controle de acesso, observando:

4.28.7.1. utilização de canais criptografados;

4.28.7.2. autenticação segura;

4.28.7.3. controle de privilégios mínimos;

4.28.7.4. registro de logs de acesso e atividades executadas;

4.28.7.5. identificação individualizada dos profissionais responsáveis pelas intervenções técnicas.

4.28.8. A CONTRATADA deverá comunicar imediatamente ao IFPI qualquer incidente de segurança da informação, vulnerabilidade crítica, comprometimento de credenciais, falha relevante ou evento que possa impactar a segurança dos ativos institucionais, apresentando:

4.28.8.1. descrição do incidente; impacto identificado; medidas corretivas adotadas; ações de mitigação implementadas.

4.28.9. A solução contratada deverá permanecer permanentemente atualizada durante toda a vigência contratual, incluindo:

4.28.9.1. assinaturas de antivírus; mecanismos de proteção; patches de segurança; atualizações corretivas; atualizações evolutivas ("updates" e "upgrades").

4.28.10. A CONTRATADA deverá assegurar que a solução permaneça suportada oficialmente pelo fabricante durante toda a vigência contratual, em versão segura e atualizada, mitigando riscos decorrentes de vulnerabilidades conhecidas.

4.28.11. A CONTRATADA deverá garantir que os mecanismos de proteção da solução possibilitem:

4.28.11.1. detecção de ameaças conhecidas e desconhecidas;

4.28.11.2. monitoramento de eventos de segurança;

4.28.11.3. geração de logs e trilhas de auditoria;

4.28.11.4. rastreabilidade das ações executadas;

4.28.11.5. proteção contra malwares, ransomwares e demais ameaças digitais.

4.28.12. Os registros de eventos e logs relacionados à solução deverão possuir mecanismos que garantam sua integridade e rastreabilidade, possibilitando auditoria e investigação de incidentes de segurança.

4.28.13. A CONTRATADA deverá observar o princípio do menor privilégio, assegurando que seus profissionais tenham acesso apenas aos recursos estritamente necessários à execução das atividades de suporte técnico.

4.28.14. Caso a execução contratual envolva tratamento de dados pessoais, a CONTRATADA deverá adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, perda, destruição, vazamento, alteração ou qualquer forma de tratamento inadequado ou ilícito, nos termos da LGPD.

4.28.15. A CONTRATADA responderá administrativa, civil e penalmente por quaisquer incidentes, danos ou prejuízos decorrentes de falhas de segurança, vazamento de informações, violação de sigilo ou tratamento inadequado de dados ocorridos durante a execução contratual.

4.28.16. O IFPI poderá, a qualquer tempo, solicitar evidências, relatórios, registros ou informações relacionadas às medidas de segurança adotadas pela CONTRATADA no âmbito da execução contratual.

4.28.17. Sempre que solicitado pela CONTRATANTE, a CONTRATADA deverá substituir imediatamente profissional que:

4.28.17.1. descumpra normas de segurança;

4.28.17.2. apresente conduta incompatível com os requisitos de confidencialidade;

4.28.17.3. represente risco à segurança da informação institucional.

4.28.18. A CONTRATADA deverá observar, ainda, as boas práticas e referências técnicas de segurança da informação aplicáveis à Administração Pública Federal, incluindo controles compatíveis com normas como ABNT NBR ISO/IEC 27001, ISO/IEC 27002 e diretrizes de gestão de riscos de segurança da informação.

Vistoria

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

Outros Requisitos Aplicáveis

4.30. Garantir a possibilidade de atualizações quando novas versões da solução forem lançadas pelo fabricante e atualização contínua das proteções contra novas ameaças digitais.

4.30.1. Aumentar a segurança para a proteção das informações tratadas no âmbito do Instituto Federal do Piauí, já que são consideradas como ativos valiosos para a eficiente prestação dos serviços públicos.

4.30.2. Criar mecanismos de manutenção a Disponibilidade, Confidencialidade e Integridade dos ativos do IFPI.

4.30.3. Redução de riscos ocasionados pela interrupção de serviços devido a ações de crackers, malwares e demais ameaças.

4.30.4. Aumentar a segurança dos sistemas informatizados do IFPI.

4.30.5. Assistência técnica especializada para os próximos anos

Sustentabilidade

4.31. 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:

4.31.1. A contratação refere-se à aquisição de licenças, que serão fornecidas pelo contratado, com prestação de serviços realizada de forma online, sem a necessidade de impressão de documentos ou materiais, assim como sem o uso de embalagens.

Indicação de marcas ou modelos

4.32. 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:

4.32.1. 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

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

4.33. Diante das conclusões extraídas do processo administrativo nº 23172.000426/2026-34, a Administração não aceitará o fornecimento dos seguintes produtos/marcas:

4.33.1. Não será admitida, durante a execução contratual, a substituição da solução atualmente utilizada por produtos, plataformas ou tecnologias incompatíveis com o ambiente institucional do IFPI, que comprometam:

4.33.1.1. a continuidade operacional da solução;

- 4.33.1.2. a compatibilidade com a infraestrutura existente;
- 4.33.1.3. o gerenciamento centralizado já implantado;
- 4.33.1.4. as políticas corporativas de segurança atualmente configuradas;
- 4.33.1.5. a integração com os ativos computacionais institucionais;
- 4.33.1.6. os mecanismos de atualização, monitoramento e resposta a incidentes já utilizados pela instituição.
- 4.33.2. A vedação prevista nesta subseção fundamenta-se:
 - 4.33.2.1. na necessidade de padronização tecnológica da solução de segurança;
 - 4.33.2.2. na preservação da continuidade administrativa e operacional;
 - 4.33.2.3. na mitigação de riscos de indisponibilidade;
 - 4.33.2.4. na manutenção da compatibilidade técnica com os ambientes já protegidos;
 - 4.33.2.5. na economicidade administrativa decorrente da manutenção da solução já implantada;
 - 4.33.2.6. na redução de impactos operacionais relacionados à migração de plataforma.
- 4.33.3. A substituição da solução atualmente utilizada por tecnologia diversa poderia acarretar:
 - 4.33.3.1. necessidade de replantação completa do ambiente de proteção;
 - 4.33.3.2. reconfiguração de políticas corporativas de segurança;
 - 4.33.3.3. indisponibilidade temporária dos mecanismos de proteção;
 - 4.33.3.4. aumento do risco de incidentes de segurança;
 - 4.33.3.5. necessidade de capacitação adicional da equipe técnica;
 - 4.33.3.6. aumento dos custos operacionais e administrativos;
 - 4.33.3.7. impacto na continuidade dos serviços institucionais suportados pela infraestrutura de TIC.
- 4.33.4. Dessa forma, somente serão aceitas soluções que mantenham plena compatibilidade técnica, operacional e funcional com o ambiente atualmente utilizado pelo IFPI, observadas as especificações e requisitos estabelecidos neste Termo de Referência e respectivos Estudos Técnicos Preliminares.
- 4.33.5. A presente vedação encontra respaldo:
 - 4.33.5.1. no art. 41, inciso III, da Lei nº 14.133/2021;
 - 4.33.5.2. no princípio da padronização previsto no art. 43 da Lei nº 14.133/2021;
 - 4.33.5.3. na necessidade de preservação da continuidade dos serviços públicos;
 - 4.33.5.4. nas diretrizes de governança e segurança da informação aplicáveis à Administração Pública Federal.

Da exigência de carta de solidariedade

4.34. Em caso de fornecedor, revendedor ou distribuidor, será exigida do licitante/interessado provisoriamente classificado em primeiro lugar, nos termos do edital ou do aviso de contratação direta, carta de solidariedade ou Termo de Parceria emitida pelo fabricante, que assegure a execução do contrato.[A20]

Subcontratação[A21]

4.35. Não será admitida a subcontratação do objeto contratual.

Da exigência de amostra

4.36. Não será exigida apresentação de amostras físicas para a presente contratação, considerando que o objeto consiste no fornecimento de licenças de software de antivírus corporativo, de natureza eminentemente digital e intangível.

4.37. Todavia, visando assegurar a compatibilidade técnica da solução ofertada com o ambiente computacional atualmente utilizado pelo Instituto Federal de Educação, Ciência e Tecnologia do Piauí – IFPI, a licitante provisoriamente classificada em primeiro lugar poderá ser convocada a apresentar, quando solicitado pela Administração, comprovação técnica da solução ofertada, mediante:

4.37.1. catálogos técnicos oficiais do fabricante;

4.37.2. datasheets;

4.37.3. documentação técnica;

4.37.4 .manuais;

4.37.5. declarações do fabricante;

4.37.6. documentação comprobatória de funcionalidades;

4.37.7. acesso controlado a ambiente demonstrativo (“demo”);

4.37.8. relatórios técnicos;

4.37.9. licenciamento de avaliação temporária, quando aplicável.

4.38. A documentação apresentada deverá comprovar o atendimento integral aos requisitos técnicos mínimos estabelecidos neste Termo de Referência, especialmente quanto:

4.38.1. à compatibilidade com ambientes Windows e Linux;

4.38.2. ao gerenciamento centralizado;

4.38.3. à proteção de estações de trabalho e servidores;

4.38.4. à atualização contínua;

4.38.5. aos mecanismos de detecção e resposta a ameaças;

4.38.6. às funcionalidades de segurança exigidas;

4.38.7. à compatibilidade com a infraestrutura tecnológica atualmente utilizada pelo IFPI.

4.38.8. A Administração poderá solicitar demonstração técnica da solução ofertada, em ambiente remoto ou presencial, exclusivamente para fins de validação funcional e verificação de conformidade técnica da solução proposta.

4.38.9. A eventual demonstração técnica não implicará instalação definitiva da solução, tampouco geração de custos adicionais para a Administração.

4.38.10. A não comprovação do atendimento aos requisitos técnicos exigidos implicará desclassificação da proposta, observadas as disposições da Lei nº 14.133/2021 e do instrumento con

4.39. As amostras poderão ser entregues no endereço Av. Jânio Quadros, Santa Isabel, TERESINA / PI, 330, CEP 64053-390, no prazo limite de 05 dias, sendo que a empresa assume total responsabilidade pelo envio e por eventual atraso na entrega.

4.40. É facultada prorrogação o prazo estabelecido, a partir de solicitação fundamentada no chat pelo interessado, antes de findo o prazo.

4.41. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita, ou havendo entrega de amostra fora das especificações previstas, a proposta será recusada.

4.42. Serão avaliados os seguintes aspectos e padrões mínimos de aceitabilidade:

4.42.1. Atender integralmente às especificações e requisitos estabelecidos neste Termo de Referência;

4.42.2. Apresentar compatibilidade com o ambiente tecnológico atualmente utilizado pelo Instituto Federal de Educação, Ciência e Tecnologia do Piauí – IFPI;

4.42.3. Comprovar funcionamento adequado das funcionalidades exigidas para proteção corporativa de endpoints;

4.42.4. Demonstrar capacidade de gerenciamento centralizado da solução;

4.42.5. Comprovar regularidade do licenciamento junto ao fabricante da solução ofertada;

4.42.6. Atender aos requisitos de suporte técnico, atualização contínua e segurança da informação previstos neste instrumento.

4.42.7. A Administração poderá solicitar documentação técnica complementar, catálogos, datasheets, demonstração funcional, acesso a ambiente de testes ou quaisquer outras informações necessárias para validação técnica da solução ofertada.

4.42.8. O não atendimento de qualquer requisito mínimo de aceitabilidade previsto neste Termo de Referência poderá ensejar a desclassificação da proposta, observadas as disposições legais, regulamentares e editais aplicáveis.

4.43. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

4.44. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), será analisada a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes neste Termo de Referência.

4.45. Os exemplares colocados à disposição da Administração serão tratados como protótipos, podendo ser manuseados e desmontados pela equipe técnica responsável pela análise, não gerando direito a ressarcimento.

4.46. Após a divulgação do resultado final do certame, as amostras entregues deverão ser recolhidas pelos fornecedores no prazo de 10 dias, após o qual poderão ser descartadas pela Administração, sem direito a ressarcimento.

4.47. Os interessados deverão colocar à disposição da Administração todas as condições indispensáveis à realização de testes e fornecer, sem ônus, os manuais impressos em língua portuguesa, necessários ao seu perfeito manuseio, quando for o caso.[A24]

Garantia da contratação[A24]

4.48. Não haverá exigência da garantia da contratação dos art. 96 e seguintes da Lei nº 14.133, de 2021, pelas razões constantes do Estudo Técnico Preliminar.

4.48.1. Não haverá exigência de garantia contratual, considerando o baixo risco operacional da contratação, a natureza continuada do licenciamento/subscrição, a inexistência de dedicação exclusiva de mão de obra, o pagamento condicionado ao ateste da execução e os mecanismos sancionatórios previstos na Lei nº 14.133/2021.

Informações relevantes para o dimensionamento da proposta

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

4.49.1. Contratação de aproximadamente 3.000 (três mil) licenças de solução corporativa de antivírus para proteção de estações de trabalho, notebooks e servidores do Instituto Federal de Educação, Ciência e Tecnologia do Piauí – IFPI;

4.49.2. Necessidade de manutenção da solução atualmente implantada no ambiente institucional, incluindo gerenciamento centralizado, atualização contínua e suporte técnico especializado;

4.49.3. Atendimento aos ambientes computacionais distribuídos entre Reitoria, campi e demais unidades administrativas do IFPI, contemplando equipamentos com sistemas operacionais Windows e Linux;

4.49.4. Necessidade de continuidade dos mecanismos de proteção contra ameaças cibernéticas, incluindo vírus, malwares, ransomwares e demais códigos maliciosos;

4.49.5. Necessidade de fornecimento de licenciamento corporativo oficial do fabricante, incluindo direito de atualização, suporte técnico e utilização durante toda a vigência contratual.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

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

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

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

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

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

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

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

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

5.2. São obrigações do CONTRATADO:

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

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

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

5.2.9. fazer a transição contratual, 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:

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

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

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

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

5.3.8. 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

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

6. MODELO DE EXECUÇÃO DO OBJETO

Condições de execução[A1]

6.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1. Início da execução do objeto: 05 dias da assinatura do contrato **OU** da emissão da ordem de serviço.

6.1.2. Descrição detalhada dos métodos, rotinas, etapas, tecnologias procedimentos, frequência e periodicidade de execução do trabalho:

6.1.2.1. fornecimento e ativação das licenças corporativas de antivírus;

6.1.2.2. renovação/subscrição da solução atualmente utilizada pelo IFPI;

6.1.2.3. *disponibilização de atualizações corretivas e evolutivas;*

6.1.2.4. *manutenção do suporte técnico especializado;*

6.1.2.5. *manutenção da compatibilidade com a infraestrutura tecnológica existente;*

6.1.2.6. *atendimento de chamados técnicos relacionados à solução;*

6.1.2.7. *suporte às atividades de administração e sustentação da plataforma de segurança.*

6.1.3. Cronograma de realização dos serviços:

6.1.3.1. Os serviços de suporte técnico deverão ser executados sob demanda, durante toda a vigência contratual, mediante abertura de chamados pela equipe técnica do IFPI, por meio de canais oficiais disponibilizados pela CONTRATADA ou pelo fabricante da solução.

6.1.4. A CONTRATADA deverá disponibilizar:

6.1.4.1. acesso às atualizações da solução;

6.1.4.2. acesso aos canais de suporte técnico;

6.1.4.3. documentação técnica oficial;

6.1.4.4. mecanismos de gerenciamento e licenciamento necessários à plena utilização da solução contratada.

Local e horário da prestação dos serviços

6.2. Os serviços serão prestados no seguinte endereço: Av. Jânio Quadros, Santa Isabel, TERESINA / PI, 330, CEP 64053-390 [A4] ;

6.3. Os serviços serão prestados no seguinte horário:

Rotinas [A4] a serem cumpridas

6.3.1. A execução contratual observará as rotinas *abaixo*:

6.3.1.1. Disponibilizar e manter ativas as licenças da solução corporativa de antivírus durante toda a vigência contratual.

6.3.1.2. Disponibilizar atualizações contínuas da solução, incluindo:

6.3.1.2. 1. *assinaturas de antivírus;*

6.3.1.2.2. *mecanismos de proteção;*

6.3.1.2.3. *patches de segurança;*

6.3.1.2.4. *atualizações corretivas;*

6.3.1.2.5. *atualizações evolutivas disponibilizadas pelo fabricante*

Materiais a serem disponibilizados

6.4. *Para a perfeita execução dos serviços, o Contratado deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário:[A5]*

6.4.1. *Para a perfeita execução dos serviços, a CONTRATADA deverá disponibilizar os recursos, licenças, acessos e meios necessários à adequada utilização da solução contratada, promovendo sua atualização ou substituição quando necessário.*

6.4.2. Licenciamento corporativo oficial da solução de antivírus, contemplando a quantidade contratada de 3.000 (três mil) licenças, com direito de uso durante toda a vigência contratual.

6.4.3. Disponibilização dos canais oficiais de suporte técnico e atendimento da solução contratada.

6.4.4. Disponibilização de acesso aos portais oficiais do fabricante ou da CONTRATADA para:

6.4.4.1. gerenciamento de licenciamento; downloads autorizados; cabertura e acompanhamento de chamados; acesso à documentação técnica; obtenção de atualizações da solução.

6.4.5. Documentação técnica oficial, manuais, guias de referência e demais informações necessárias à adequada utilização da solução pelo IFPI.

6.4.6. Ferramentas e mecanismos necessários à manutenção da compatibilidade da solução com o ambiente tecnológico institucional.

Informações relevantes para o dimensionamento da proposta

6.5. A demanda do órgão tem como base as seguintes características:[A6]

6.5.1. Contratação de 3.000 (três mil) licenças de solução corporativa de antivírus destinadas à proteção dos ativos computacionais do Instituto Federal de Educação, Ciência e Tecnologia do Piauí – IFPI.

6.5.2. A solução deverá atender ambientes corporativos compostos por: estações de trabalho; notebooks; servidores; equipamentos conectados à rede institucional.

Formas de transferência de conhecimento

6.6. Não será necessária transferência de conhecimento devido às características do objeto.

Procedimentos de transição e finalização do contrato

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

Quantidade mínima de serviços para comparação e controle

6.8. Cada OS conterá o volume de serviços demandados, incluindo a sua localização e o prazo, conforme modelo descrito no [Anexo].

Mecanismos formais de comunicação

6.9. 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;

Manutenção de Sigilo e Normas de Segurança

6.10. 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.

6.11. 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.

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 o preposto da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

7.5. O Contratado designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto Contratado.

7.6. O Contratado *não necessitará* manter preposto da empresa no local da execução do objeto *durante o período de 36 meses*.

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

Reunião Inicial

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

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

7.10. A pauta desta reunião observará, pelo menos:

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

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

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

7.10.4. 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;

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

Rotinas de Fiscalização

7.11. 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

- 7.12. O fiscal técnico do contrato 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.
- 7.13. O fiscal técnico do contrato anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.
- 7.14. Identificada qualquer inexecução ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.
- 7.15. 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.
- 7.16. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprezadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.
- 7.17. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual.
- 7.18. *A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:*
- 7.18.1. Verificar a manutenção da validade e regularidade das licenças da solução corporativa de antivírus durante toda a vigência contratual.
- 7.18.2. Acompanhar a disponibilização das atualizações da solução, incluindo:
- 7.18.2.1. assinaturas de antivírus;
 - 7.18.2.2. mecanismos de proteção;
 - 7.18.2.3. patches de segurança;
 - 7.18.2.4. atualizações corretivas;
 - 7.18.2.5. atualizações evolutivas disponibilizadas pelo fabricante.
- 7.18.2. Monitorar a prestação do suporte técnico fornecido pela CONTRATADA, especialmente quanto:
- 7.18.2.1. aos prazos de atendimento;
 - 7.18.2.2. à qualidade das respostas técnicas;
 - 7.18.2.3. à resolução de incidentes;
 - 7.18.2.4. ao atendimento das demandas encaminhadas pela equipe técnica do IFPI.
- 7.18.3. Verificar a compatibilidade e continuidade operacional da solução no ambiente computacional institucional.
- 7.18.4. Acompanhar o funcionamento dos mecanismos de gerenciamento centralizado da solução.
- 7.18.5. Verificar a regularidade dos canais de suporte técnico e atendimento disponibilizados pela CONTRATADA.
- 7.18.6. Registrar ocorrências, falhas, indisponibilidades, incidentes ou descumprimentos contratuais eventualmente identificados durante a execução do contrato.
- 7.18.7. Solicitar à CONTRATADA correções, esclarecimentos ou providências necessárias ao adequado cumprimento das obrigações contratuais.
- 7.18.8. Verificar o cumprimento das obrigações relacionadas à segurança da informação e proteção de dados previstas neste Termo de Referência.

7.18.9. Atestar o recebimento dos serviços executados e autorizar os procedimentos de pagamento, observadas as condições estabelecidas neste instrumento.

7.19. 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 do Contratante ou de seus agentes, gestores e fiscais, de conformidade.

Fiscalização Administrativa

7.20. 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.

7.21. 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.

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

7.22.1. *Realizar acompanhamento contínuo da execução contratual, verificando o cumprimento das obrigações previstas neste Termo de Referência, no contrato e na proposta da CONTRATADA.*

7.22.2. *Verificar a disponibilidade e continuidade dos serviços de suporte técnico e atualização da solução durante toda a vigência contratual.*

7.22.3. *Acompanhar a regularidade do licenciamento da solução junto ao fabricante, incluindo vigência, atualização e suporte oficial.*

7.22.4. *Verificar a manutenção das funcionalidades de gerenciamento centralizado e proteção dos ativos computacionais institucionais.*

7.22.5. *Registrar em processo administrativo próprio todas as ocorrências relevantes relacionadas à execução contratual, incluindo falhas, indisponibilidades, notificações e eventuais descumprimentos contratuais.*

7.22.6. *Solicitar formalmente à CONTRATADA a adoção de medidas corretivas sempre que identificadas falhas na execução contratual.*

7.22.7. *Subsidiar a Administração com informações necessárias à aplicação de sanções, glosas, advertências ou demais medidas administrativas previstas contratualmente, quando cabíveis.*

7.22.8. *Avaliar periodicamente a conformidade da solução com os requisitos técnicos, operacionais e de segurança definidos neste Termo de Referência.*

Gestor do Contrato

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

7.23.1. 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.

7.23.2. 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.

7.23.3. acompanhar a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.23.4. 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.

7.23.5. 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.

7.23.6. 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.

7.23.7. enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, com a indicação expressa de que o valor da Nota Fiscal emitida pela contratada confere com o valor dimensionado pela fiscalização e gestão no recebimento definitivo do serviço.

7.23.8. receber e dar encaminhamento imediato:

7.23.8.1. às denúncias de discriminação, violência e assédio no ambiente de trabalho, conforme o art. 2º, inciso III, do Decreto n.º 12.174/2024;

7.23.8.2. à notificação formal de que a empresa contratada está descumprindo suas obrigações trabalhistas, enviada pelo trabalhador, sindicato, Ministério do Trabalho, Ministério Público, Defensoria Pública ou por qualquer outro meio idôneo.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), conforme disposto nesta seção.

IAP – ÍNDICE DE ATENDIMENTO NO PRAZO	
Tópico	Descrição
Finalidade	Medir o tempo de atraso na prestação dos serviços constantes na Ordem de Serviço.
Meta a cumprir	IAP igual ou superior a 95 %.
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
Forma de acompanhamento	É apurado pelos fiscais do contrato avaliando a quantidade atendida dentro do prazo em relação à quantidade total atendida no período de referência.

Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	$IAP = 100 * (\Sigma Q_{tap} / \Sigma Q_{tr})$ Onde: <i>IAP = Indicador de atendimento aos prazos do serviço;</i> <i>ΣQ_{tap} = Somatório do quantitativo atendido no prazo máximo estabelecido no TR com previsão de encerramento para o período de referência;</i> <i>ΣQ_{tr} = Somatório do quantitativo total registrado com previsão de encerramento para o período de referência.</i>
Observações	<i>Obs1: Serão utilizados dias corridos na medição.</i> <i>Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.</i>
Início de Vigência	A partir da emissão da OS.
Faixas de ajuste no pagamento e Sanções	<i>IAP >= 90%: sem descontos sobre o valor da fatura mensal.</i> <i>IAP >= 80% e < 90%: 10% de desconto sobre o valor da fatura mensal.</i> <i>IAP >= 70% e < 80%: 20% de desconto sobre o valor da fatura mensal.</i> <i>IAP < 70%: 30% de desconto sobre o valor da fatura mensal.</i>

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

8.2.1. não produziu os resultados acordados,

8.2.2. deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou

8.2.3. deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou os utilizou com qualidade ou quantidade inferior à demandada.

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

8.4. A aferição[A1] da execução contratual para fins de pagamento considerará os seguintes critérios:

8.4.1. Comprovação da disponibilização e manutenção das licenças da solução corporativa de antivírus durante o período de referência do faturamento.

8.4.2. Comprovação da regularidade do licenciamento da solução junto ao fabricante, incluindo direito de atualização e suporte técnico.

8.4.3. Disponibilização das atualizações da solução, incluindo: assinaturas de antivírus; mecanismos de proteção; patches de segurança; atualizações corretivas e evolutivas.

8.4.4. Comprovação da prestação dos serviços de suporte técnico previstos contratualmente.

8.4.5. Verificação do cumprimento dos níveis mínimos de serviço eventualmente estabelecidos para atendimento de chamados técnicos.

8.4.6. Ausência de falhas graves, indisponibilidades injustificadas ou descumprimentos contratuais que comprometam a utilização da solução no ambiente institucional do IFPI.

8.4.7. Comprovação de que a solução permaneceu oficialmente suportada pelo fabricante durante o período de execução contratual correspondente.

8.4.8. Cumprimento das obrigações relacionadas à segurança da informação e proteção de dados previstas neste Termo de Referência.

Recebimento

8.5. Os serviços serão recebidos provisoriamente, no prazo de 05 dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

8.6. O prazo para recebimento provisório será contado do recebimento de comunicação de cobrança oriunda do Contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

8.7. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

8.8. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

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

8.10. Para efeito de recebimento provisório, será considerado para fins de faturamento o período de 5 (cinco) dias. .

8.11. Ao final de cada período/evento de faturamento:

8.11.1. o fiscal técnico do contrato deverá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato;

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

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

8.14. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no recebimento provisório.

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

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

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

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

8.18.1 Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento.

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

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

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

8.18.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.[A5]

8.19. 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.

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

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

Procedimentos de Teste e Inspeção

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

8.22.1. Verificação da disponibilização e ativação das licenças contratadas, observando: quantitativo contratado; vigência das licenças; regularidade junto ao fabricante; compatibilidade com o ambiente institucional do IFPI.

8.22.2. Validação do acesso aos serviços de suporte técnico, incluindo: canais de atendimento; abertura de chamados; acompanhamento de ocorrências; disponibilidade dos meios oficiais de suporte.

8.22.3. Verificação da disponibilidade das atualizações da solução, incluindo: assinaturas de antivírus; mecanismos de proteção; patches de segurança; atualizações corretivas e evolutivas disponibilizadas pelo fabricante.

8.22.4. Verificação do funcionamento da solução no ambiente computacional institucional, especialmente quanto: à proteção dos endpoints; ao gerenciamento centralizado; à comunicação com a console de gerenciamento; à atualização dos agentes instalados.

8.22.5. Análise da compatibilidade da solução com os sistemas operacionais utilizados no IFPI, incluindo ambientes Windows e Linux.

8.22.6. *Verificação da geração de logs, eventos e relatórios relacionados à proteção dos ativos computacionais.*

8.22.7. *Validação do atendimento aos requisitos técnicos, operacionais e de segurança estabelecidos neste Termo de Referência.*

8.22.8. *Análise da documentação técnica, comprovantes de licenciamento, registros de suporte e demais evidências necessárias ao recebimento contratual.*

Liquidação

8.23. 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.

8.24. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos 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.

8.25. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

- I) o prazo de validade;
- II) a data da emissão;
- III) os dados do contrato e do órgão contratante;
- IV) o período respectivo de execução do contrato;
- V) o valor a pagar; e
- VI) eventual destaque do valor de retenções tributárias cabíveis.

8.26. Havendo erro na apresentação da Nota Fiscal/Fatura, 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.

8.27. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada 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 14.133/2021.

8.28. A Administração deverá realizar consulta ao SICAF para:

8.28.1. verificar a manutenção das condições de habilitação exigidas;

8.28.2. 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.

8.29. 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.

8.30. 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.

8.31. 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.

8.32. 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

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

8.34. 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 IPCA - Índice Nacional de Preços ao Consumidor Amplo de correção monetária.

Forma de pagamento

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

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

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

8.37.1. 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.[A7]

8.38. 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.

Antecipação de pagamento

8.39. *Não será admitido pagamento antecipado, tendo em vista que a execução contratual permite a adequada aferição do cumprimento das obrigações pela CONTRATADA previamente à realização do pagamento, observados os princípios da eficiência, economicidade e segurança da contratação pública.*

Reajuste

8.40. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 01/06/2026

8.41. 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.

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

8.43. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

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

8.45. 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.

8.46. 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.

8.47. O reajuste será realizado por apostilamento.

Cessão de Crédito

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

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

8.48.2. 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.

8.48.3. 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.

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

8.49. 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.[A20]

9. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

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

<i>Id</i>	<i>Ocorrência</i>	<i>Glosa / Sanção</i>
1	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 24 horas úteis.	Multa de 0.2 % sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela contratante, até o limite de 5 dias úteis.
		Após o limite de 5 dias úteis, aplicar-se-á multa de 2 % do valor total do Contrato.
2	Não atender ao indicador de nível de serviço IAP (Índice de Atendimento no Prazo)	IAP >= 90%: sem descontos sobre o valor da fatura mensal.
		IAP >= 80% e < 90%: 10% de desconto sobre o valor da fatura mensal.
		IAP >= 70% e < 80%: 20% de desconto sobre o valor da fatura mensal.
		IAP < 70%: 30% de desconto sobre o valor da fatura mensal.

3	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	<i>Advertência.</i> <i>Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 2 % do valor total do Contrato.</i>
---	--	---

9.2. 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 p contratado:

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

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

9.3. 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.

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

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

9.4.2. 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;

9.4.3. 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.

9.4.4. Multa:

9.4.4.1. Moratória, para as infrações descritas no item “d”, de **0,5%** por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de **10 dias**.

9.4.4.2. Moratória de 0,07% (sete centésimos 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;

9.4.4.2.1. O atraso superior a 25 (vinte e cinco) 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.

9.4.4.3. Compensatória, para as infrações descritas acima alíneas “e” a “h” de **5% (cinco por cento) a[A4] 10% (dez por cento) do valor da contratação**.

9.4.4.4. *Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de 10% (dez por cento) a 20% (vinte por cento) do valor da contratação.*

9.4.4.5. *Compensatória, para a infração descrita acima na alínea “b”, de 2% (dois por cento) a 5% (cinco por cento) do valor da contratação.*

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

9.4.4.7. *Compensatória, para a infração descrita acima na alínea “a”, de 2% (dois por cento) a 5% (cinco por cento) do valor da contratação [, ressalvadas as seguintes infrações também enquadráveis nessa alínea:]*

9.4.4.7.1.1. *Não disponibilizar atualizações de assinaturas, mecanismos de proteção ou patches de segurança da solução durante a vigência contratual.*

9.4.4.7.1.2. *Interromper injustificadamente o suporte técnico contratado ou deixar de atender chamados técnicos dentro dos prazos estabelecidos.*

9.4.4.7.1.3. *Permitir a expiração, suspensão ou irregularidade das licenças fornecidas ao IFPI durante a vigência contratual.*

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

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

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

9.8. 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.

9.9. A multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

9.10. 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.

9.10.1. 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.

9.10.2. 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.

9.11. Na aplicação das sanções serão considerados:

9.11.1. a natureza e a gravidade da infração cometida;

9.11.2. as peculiaridades do caso concreto;

9.11.3. as circunstâncias agravantes ou atenuantes;

9.11.4. os danos que dela provierem para o Contratante; e

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

9.12. 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.

9.13. 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.

9.14. 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.

9.14.1. As penalidades serão obrigatoriamente registradas no SICAF.

9.15. 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.

9.16. 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.

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

Forma de seleção e critério de julgamento da proposta

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

Regime de Execução

10.2. O regime de execução do contrato será por 36 meses.

Exigências[A4] de habilitação

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

Habilitação jurídica

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

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

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

- 10.7. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;
- 10.8. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.
- 10.9. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;
- 10.10. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;
- 10.11. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.
- 10.12. Consórcio de empresas: contrato de consórcio devidamente arquivado no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis (art. 279 da Lei nº 6.404, de 15 de dezembro de 1976) ou compromisso público ou particular de constituição, subscrito pelos consorciados, com a indicação da empresa líder, responsável por sua representação perante a Administração (art. 15, caput, I e II, da Lei nº 14.133, de 2021).
- 10.14. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

- 10.15. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;
- 10.16. 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.
- 10.17. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
- 10.18. 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;
- 10.19. Prova de inscrição no cadastro de contribuintes Distrital ou Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- 10.20. Prova de regularidade com a Fazenda Distrital ou Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
- 10.21. 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.
- 10.22. 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

- 10.23. 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;
- 10.24. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;
- 10.25. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis *dos 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[A11] :

LG =

Ativo Circulante + Realizável a Longo Prazo

Passivo Circulante + Passivo Não Circulante

SG =

Ativo Total

Passivo Circulante + Passivo Não Circulante

LC =

Ativo Circulante

Passivo Circulante

- 10.27. Caso a empresa apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido, para fins de habilitação, **[capital mínimo] OU [patrimônio líquido mínimo]** de **[definir percentual, limitado a 10%]** do **[valor total estimado da contratação]**.
- 10.28. Os indicadores fixados acima deverão ser atingidos em cada um dos dois últimos exercícios sociais, sob pena de inabilitação;
- 10.29. 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;
- 10.30. 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.
- 10.31. O atendimento dos índices econômicos previstos neste termo de referência deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.
- 10.32. 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

- 10.33. Declaração de que o fornecedor tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da contratação.

10.33.1. Essa declaração poderá ser substituída por declaração formal assinada pelo responsável técnico do interessado acerca do conhecimento pleno das condições e peculiaridades da contratação.

10.33.1. Para efeito de qualificação técnica, a LICITANTE deve demonstrar sua aptidão e capacidade técnico operacional para a execução do OBJETO mediante comprovação de prestação bem-sucedida de fornecimento de bens e de serviços em características compatíveis com a presente licitação, mediante apresentação de um ou mais ATESTADO(S) DE CAPACIDADE TÉCNICA que deverão comprovar o fornecimento de, no mínimo, 50% (cinquenta por cento) do volume estimado para o item em disputa e com características compatíveis com o objeto da presente pretensão contratual, incluindo garantia e assistência técnica podendo considerar contratos já executados e/ou em execução.

10.33.2. Os atestados apresentados deverão comprovar que a licitante executou, no mínimo, 50% (cinquenta) das quantidades das parcelas de maior relevância técnica, conforme definido no Art. 67, § 2º da Lei nº 14.133, de 2021 e fundamentada no art. 37, inciso XXI, da Constituição Federal.

10.33.4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

10.33.5. Deve ser apresentado atestado de capacidade técnica ou declaração emitida pelo fabricante da solução, comprovando que a licitante é apta a configurar, prestar suporte técnico e ministrar treinamentos das soluções referente a este edital

10.33.6. A contratada deverá possuir, pelo menos, um técnico certificado pelo fabricante compatível com o objeto deste termo de referência.

10.33.7. A comprovação de vínculo profissional se fará com a apresentação de cópia da carteira de trabalho (CTPS) em que conste o licitante como contratante; do contrato social do licitante em que conste o profissional como sócio; do contrato de prestação de serviços, sem vínculo trabalhista, regido pela legislação civil ou, ainda, de declaração de contratação futura do profissional, desde que acompanhada de declaração de anuência do profissional.

10.33.8. A empresa licitante deverá obrigatoriamente comprovar que é revenda credenciada pelo fabricante e que está apta a comercializar seus produtos;

10.34. Sociedades empresárias estrangeiras atenderão à exigência por meio da apresentação, no momento da assinatura do contrato ou do aceite de instrumento equivalente, da solicitação de registro perante a entidade profissional competente no Brasil.

10.35. Comprovação de aptidão para execução de serviço similar, 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[A18] .

10.35.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contrato(s) executado(s) com as seguintes características mínimas:[A19]

10.35.1.1. contrato(s) que comprove(m) a experiência mínima de 1 (um) ano do fornecedor na prestação dos serviços, em períodos sucessivos ou não, sendo aceito o somatório de atestados de períodos diferentes:[A20]

10.35.2. [A21] Serão admitidos, para fins de comprovação de quantitativo mínimo de serviço, a apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante.

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

10.35.4. O fornecedor disponibilizará [A24] 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 foram prestados os serviços, entre outros documentos.

10.35.5. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

10.36. Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

10.37. A apresentação, pelo fornecedor, de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitida, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133/2021 e regulamentos sobre o tema.

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

Disposições gerais sobre habilitação

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

10.41. 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.

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

10.43. 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.

10.44. 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.

Documentação complementar para cooperativas

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

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

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

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

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

10.45.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;

10.45.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:

10.45.6.1. ata de fundação;

10.45.6.2. estatuto social com a ata da assembleia que o aprovou;

10.45.6.3. regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;

10.45.6.4. editais de convocação das três últimas assembleias gerais extraordinárias;

10.45.6.5. três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas

reuniões seccionais;

10.45.6.6. ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da contratação; e

10.45.6.7. última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador[A26] .

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação, que é o máximo aceitável, é de R\$ 570.780,00 (quinhentos e setenta mil e setecentos e oitenta reais), conforme custos unitários apostos na **[tabela contida no item 1.1 acima]**.

11.5. 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, das obras ou dos serviços registrados, nas seguintes situações:

11.5.1. 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;

11.5.2. 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;

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

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

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. A indicação da dotação orçamentária fica postergada para o momento da assinatura do contrato.

13. DISPOSIÇÕES FINAIS

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

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](#).

NATANAEL RIBEIRO DA SILVA

Integrante requisitante



Assinou eletronicamente em 17/09/2026 às 10:39:33.

LUCAS FERNANDES RIBEIRO

Integrante técnico substituto



Assinou eletronicamente em 17/09/2026 às 09:25:23.

ANTONIO FRANCISCO MARTINS FORTES

Integrante administrativo



Assinou eletronicamente em 17/09/2026 às 10:02:17.

LARISSA SANTIAGO DE AMORIM

Autoridade competente



Assinou eletronicamente em 18/09/2026 às 09:53:08.