

MODELO DE TERMO DE REFERÊNCIA
Lei nº 14.133, de 1º de abril de 2021
LICITAÇÃO



Instituto Federal do Sertão Pernambucano

(Processo Administrativo nº 23302.101823/2025-19)

TERMO DE REFERÊNCIA

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. O presente Termo de Referência consiste na contratação de Serviço de Fornecimento de Licenças para Solução Integrada de Proteção de Rede para Segurança da Informação: Next Generation Firewall (NGFW) pelo período de 60 (sessenta) meses e cessão temporária de direitos sobre programas de computador referente à locação do pacote de softwares AUTODESK AEC – Architecture, Engineering and Construction Collection pelo período de 36 (trinta e seis) meses. Conforme especificações e condições constantes deste:

Objeto: Contratação de Licenças de Proteção de Rede para Segurança de Informação (NGFW) e Software CAD						
Grupo 01: Licença para Solução Integrada de Proteção de Rede para Segurança da Informação: NGFW						
Item	Especificação	CATSER	Métrica ou Unidade de Medida	Quantidade	Valor Unitário (R\$)	Valor Total (R\$)
1	Serviço de Fornecimento de Licença para Solução Integrada de Proteção de Rede para Segurança da Informação: Next Generation Firewall (NGFW) – Tipo 1 com atualização por 60 (sessenta) meses. Part Number: FC2-10-FGVS-990-02-60 CATSer: 27502	27502	Unidade	5	111.500,40	557.502,00
2	Serviço de Fornecimento de Licença para Solução Integrada de Proteção de Rede para Segurança da Informação: Next Generation Firewall (NGFW) – Tipo 2 com atualização por 60 (sessenta) meses. Part Number: FC3-10-FGVS-990-02-60 CATSer: 27502	27502	Unidade	2	206.528,00	413.056,00
3	Serviço de Fornecimento de Licença para Solução Integrada de Proteção de Rede para Segurança da Informação: Next Generation	27502	Unidade	2	501.194,30	1.002.388,60

	Firewall (NGFW) – Tipo 3 com atualização por 60 (sessenta) meses. Part Number: FC4-10-FGVS-990-02-60 CATSer: 27502					
4	Licença para solução integrada de proteção de rede para segurança da informação: Software de coleta e análise de logs centralizado com atualização por 60 meses. Part Number: FC1-10-FGVS-258-01-60 CATSer: 27502	27502	Unidade	1	23.079,75	23.079,75
5	Licença para solução integrada de proteção de rede para segurança da informação: Software de gerenciamento centralizado com atualização por 60 meses. Part Number: FC1-10-AZVMS-465-01-60 CATSer: 27502	27502	Unidade	1	45.250,00	45.250,00
6	Serviço de Instalação, configuração e repasse de conhecimento. CATSer: 26972	26972	Unidade	6	22.750,00	136.500,00
Valor Total Estimado da Contratação (Grupo 01)						2.177.776,35

Grupo 02: Software CAD						
Item	Especificação	CATSER	Métrica ou Unidade de Medida	Quantidade	Valor Unitário (R\$)	Valor Total (R\$)
07	Autodesk AutoCAD LT	27502	Unidade	04	8.085,58	32.342,32
08	Autodesk Architecture, Engineering & Construction Collection (AEC Collection)	27502	Unidade	02	49.999,00	99.998,00
Valor Total Estimado da Contratação (Grupo 02)						132.340,32
Valor Total Estimado da Contratação (Grupos 01 e 02)						2.310.116,67

A contratação será realizada por meio do Sistema de Registro de Preços – SRP, nos termos do art. 82 da Lei nº 14.133/2021 e do Decreto nº 11.462/2023.

A contratação em lote justifica-se pela racionalização do processo administrativo, ganho de escala e simplificação da gestão contratual.

Classificação do objeto quanto à heterogeneidade ou complexidade

1.2. O(s) serviço(s) objeto desta contratação são caracterizados como **comum**, 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 uma necessidade permanente da IFSertãoPE, sendo a; vigência plurianual mais vantajosa considerando Estudo Técnico Preliminar.

Prazo de vigência

1.4. O prazo de vigência da contratação é de 60 (sessenta) meses para os itens do Grupo 01 e de 36 (Trinta e seis) meses do grupo 02.

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.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. O Instituto Federal do Sertão Pernambucano (IFSertãoPE), composto por sete unidades acadêmicas e pela Reitoria, atende atualmente cerca de 12.000 usuários, entre alunos, professores e servidores técnico-administrativos. Para garantir a continuidade dos serviços educacionais e administrativos com segurança, é essencial que a infraestrutura de Tecnologia da Informação esteja equipada com soluções robustas e atualizadas de proteção de rede.

A aquisição das licenças da solução integrada de segurança FortiGate – Next Generation Firewall (NGFW) da Fortinet – representa um passo estratégico na modernização da política de segurança da informação da Instituição. Essa solução oferece recursos avançados de inspeção de tráfego, controle de aplicações, prevenção contra ameaças, filtragem de conteúdo, VPN segura e visibilidade detalhada da rede, permitindo uma gestão proativa e inteligente dos riscos cibernéticos.

Atualmente, o IFSertãoPE opera com licenças algumas vencidas e outras próximas a se vencer, o que limita significativamente a capacidade de monitoramento e defesa contra-ataques, além de comprometer a eficiência da rede. Com a renovação e ampliação das licenças para todas as unidades e a Reitoria, será possível:

- Reforçar a segurança da rede institucional, protegendo dados sensíveis e sistemas críticos utilizados em processos acadêmicos e administrativos.
- Monitorar e controlar o tráfego de rede em tempo real, identificando comportamentos suspeitos e prevenindo incidentes antes que causem danos.
- Garantir a integridade dos sistemas educacionais e administrativos, que concentram informações estratégicas para a gestão e a tomada de decisões.
- Melhorar a performance e a estabilidade da conexão, otimizando o uso da banda larga e reduzindo gargalos que afetam o acesso a serviços digitais.
- Proporcionar um ambiente digital mais seguro para toda a comunidade acadêmica, promovendo confiança no uso de recursos tecnológicos por alunos, docentes e servidores.

A implementação da solução FortiGate NGFW contribuirá diretamente para a continuidade dos serviços institucionais com maior resiliência, eficiência e segurança, alinhando-se às melhores práticas de governança de TI e proteção de dados. Portanto, a aquisição das licenças é não apenas necessária, mas estratégica para garantir a proteção da infraestrutura digital do IFSertãoPE e para promover um ambiente acadêmico mais seguro, confiável e moderno.

Em relação a contratação dos softwares de CAD é de fundamental importância para o Instituto Federal do Sertão Pernambucano (IFSertãoPE), em especial para o setor de Engenharia, considerando os seguintes aspectos:

- **Atendimento às demandas institucionais:** Os projetos de infraestrutura física do IFSertãoPE exigem o uso de softwares de desenho assistido por computador (CAD) para elaboração, revisão e

atualização de plantas arquitetônicas, elétricas, hidrossanitárias e estruturais. Esses projetos são indispensáveis para construção, reformas, ampliações e manutenção das unidades do Instituto.

- **Conformidade técnica e padronização:** O uso de softwares CAD garante a padronização dos desenhos técnicos conforme normas da ABNT e demais regulamentos vigentes, assegurando precisão nas informações e compatibilidade entre diferentes disciplinas da engenharia.
- **Eficiência e produtividade:** Os softwares possibilitam maior agilidade na elaboração e alteração de projetos, reduzindo tempo de execução, evitando retrabalho e melhorando a qualidade da documentação técnica.
- **Suporte a órgãos de controle e fiscalização:** A correta elaboração e arquivamento dos projetos em formato eletrônico padronizado permite maior transparência e rastreabilidade, atendendo às exigências de órgãos de controle interno e externo.
- **Integração com outras áreas:** A utilização desses softwares possibilita a integração entre a equipe de engenharia, arquitetos, técnicos de edificações e setores administrativos, viabilizando a execução de projetos de forma colaborativa e eficiente.
- **Modernização e atualização tecnológica:** A contratação garante que o IFSertãoPE disponha de ferramentas atualizadas e compatíveis com o mercado, promovendo a modernização da infraestrutura de trabalho da equipe de engenharia e alinhando-se às melhores práticas da área.

Diante da necessidade de elaborar e gerenciar projetos de engenharia de forma precisa, ágil e padronizada, a contratação dos softwares CAD é essencial para assegurar a continuidade e qualidade das atividades do setor de Engenharia do IFSertãoPE, trazendo benefícios diretos à gestão institucional e ao atendimento das demandas acadêmicas e administrativas.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2026, conforme detalhamento a seguir:

- ID PCA no PNCP: [10830301000104-0-000009/2025];
- Data de publicação no PNCP: [13/05/2024];
- Id do item no PCA: [22];
- Classe/Grupo: [182 - SERVIÇOS DE LICENCIAMENTO E CONTRATOS DE TRANSFERÊNCIA DE TECNOLOGIA];
- Identificador da Futura Contratação: [158149-27/2025];

2.3. 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) 2025/2026 do Instituto Federal do Sertão Pernambucano (IFSertãoPE), conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos
PDI - OE01	Aprimorar a infraestrutura física e tecnológica

ALINHAMENTO AO PDTIC 2025/2026	
ID	Necessidade do PDTIC
N25	Aquisição de Software para Segurança da Informação (Antivírus, Firewall UTM, etc.)
N30	Aquisição de Licenças de Software para Gestão, Ensino, Pesquisa e Extensão (Microsoft, Adobe, Autodesk, Google, entre outros)

2.4. ~~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 na contratação de Empresa Especializada para Prestação de Serviço de Fornecimento de Licenças para Solução Integrada de Proteção de Rede para Segurança de Informação: Next Generation Firewall (NGFW) pelo período de 60 (sessenta) meses e cessão temporária de direitos sobre programas de computador referente à locação do pacote de softwares AUTODESK AEC – Architecture, Engineering and Construction Collection pelo período de 36 (trinta e seis) meses.

3.3. Todos os itens que compõem a solução deverão ser compatíveis com o atual ambiente em produção do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO, de forma que seja mantida a operabilidade com todos os recursos atualmente utilizados e para que não haja impacto na operação da rede e segurança da CONTRATANTE.

3.4. Deverão ser apresentados juntamente com a proposta comercial os CATÁLOGOS, ENCARTES, FOLHETOS TÉCNICOS E SEUS RESPECTIVOS MANUAIS que deverão compor todos os itens ofertados permitindo a consistente avaliação dos itens e serviços.

Grupo 01	ITEM	ESPECIFICAÇÃO	CATSER	TOTAL
	01	Serviço de Fornecimento de Licença para Solução Integrada de Proteção de Rede para Segurança de Informação: Next Generation Firewall (NGFW) – Tipo 1 com atualização por 60 (sessenta) meses. Part Number: FC2-10-FGVVS-990-02-60	27502	5
	02	Serviço de Fornecimento de Licença para Solução Integrada de Proteção de Rede para Segurança de Informação: Next Generation Firewall (NGFW) – Tipo 2 com atualização por 60 (sessenta) meses. Part Number: FC3-10-FGVVS-990-02-60	27502	2
	03	Serviço de Fornecimento de Licença para Solução Integrada de Proteção de Rede para Segurança de Informação: Next Generation Firewall (NGFW) – Tipo 3 com atualização por 60 (sessenta) meses. Part Number: FC4-10-FGVVS-990-02-60	27502	2
	04	Licença para solução integrada de proteção de Rede para segurança de informação: Software de coleta e análise de logs centralizado com atualização por 60 (sessenta) meses. Part Number: FC1-10-FMGVS-258-01-60	27502	1
	05	Licença para solução integrada de proteção de Rede para segurança de informação: Software de gerenciamento centralizado com atualização por 60 (sessenta) meses.	27502	1

		Part Number: FC2-10-AZVMS-465-01-60		
	06	Serviço de Instalação, configuração e repasse de conhecimento	26972	6

Grupo 02	ITEM	ESPECIFICAÇÃO	CATSER	TOTAL
	07	Autodesk AutoCAD LT	27502	4
	08	Autodesk Architecture, Engineering & Construction Collection (AEC Collection)	27502	2

Descrição Detalhada

Item	Descrição
01	Firewall UTM – Tipo 1 - VM2 O objeto aqui definido como “Firewall UTM” é também referenciado no mercado como Firewall de Última Geração – Next-Generation Firewall – (NGFW). Esses termos diversos poderão ser utilizados durante a descrição deste item, incluindo seus usos substanciados, como Firewall, UTM, NGFW, plataforma, equipamento ou mesmo appliance. REQUISITOS GERAIS O Firewall UTM poderá ser instalado nas seguintes plataformas de virtualização: VMware ESXi (6.0) e KVM (versão disponível nos repositórios oficiais do CentOS 7). A imagem para instalação do appliance deverá ser fornecida em formato compatível com ambas as plataformas de virtualização. Deverá estar licenciado para no mínimo 2 (dois) vCPU cores. Deve possuir sistema operacional próprio preparado para atender serviços essenciais de segurança (Firewall, VPN, IPS). Este sistema operacional deve implementar uma interface gráfica web (usando http / https) que permite que todas as funções do sistema operacional e configurações tradicionais sejam realizadas, incluindo funções de troubleshooting. O Sistema Operacional do firewall deve ser capaz de adicionar novas funcionalidades sem a necessidade de reinstalação da solução. Os componentes da solução (incluindo o sistema operacional, drivers de dispositivos e aplicativos de segurança) devem ser desenvolvidos, produzidos e comercializados pela mesma fabricante. Deve implementar, diretamente no firewall ou na solução de gerenciamento centralizado a segmentação de acessos administrativos, permitindo que os administradores façam modificações nas configurações, relatórios e logs de maneira independente, sem que uma comprometa a outra. O sistema operacional do appliance deve suportar autenticação de usuários externa, através do protocolo RADIUS e/ou LDAP, e não deve exigir contas de usuário local a ser criado no sistema operacional, com exceção de um administrador para uso em caso de falha de comunicação com os servidores de autenticação externos. A solução deve ter integração com diretórios LDAP para autenticação e autorização de usuários baseado nos perfis armazenados no LDAP ou no firewall. Deve incluir a funcionalidade de pesquisar múltiplos servidores de LDAP para redundância e encontrar usuários distribuídos em múltiplos servidores de LDAP. O sistema operacional deve implementar política de senha de usuário administrador, com os seguintes requisitos: • Deve ser capaz de impor um tamanho mínimo e os diferentes tipos de caracteres (números, letras, caracteres especiais); • Deve ser capaz de forçar mudanças de senha periódica; • Deve acompanhar o histórico de senhas “velhas” para evitar a reutilização delas; • Deve implementar o bloqueio de conta de usuário depois de várias tentativas de login sem sucesso; • Deve implementar o bloqueio de conta de usuário após dias sem tentativas de login por longos períodos de tempo. A configuração do sistema operacional e monitoramento do mesmo deve suportar a administração baseada em perfis de acesso por grupo e/ou usuário.

Item	Descrição
	O sistema operacional deve suportar configurar um disclaimer (aviso legal) na tela de login do administrador do sistema operacional (NGFW). O sistema operacional deve suportar arquiteturas de clusters implementadas com balanceadores de carga (Load Balance). Deve suportar configurações de cluster e Alta Disponibilidade (High Availability - HA) que, em caso de falha de um dos nós do cluster, o impacto não seja perceptível para os utilizadores e as aplicações em modos ativo/standby e ativo/ativo na arquitetura implementada. O appliance deve suportar à gestão remota segura através da rede utilizando protocolo SSH e HTTPS, independente de software adicional. Suas interfaces de rede devem suportar VLANs (802.1Q e Trunking), assim como o tráfego non-tagged. Todos os componentes e processos críticos do sistema operacional devem gerar logs e suportar log remoto através do protocolo syslog, bem como utilizar o protocolo SNMP (versões 2 e 3), incluindo suporte traps de falhas e eventos. O sistema operacional deve possuir ferramenta de resolução de problemas em tempo real filtrando a captura de tráfego e armazenando-a, podendo exportá-la em formato compatível com a biblioteca libpcap. As configurações do sistema poderão ser exportadas como forma de backup sob demanda ou por agendamento para locais externos ao armazenamento do próprio appliance. O sistema operacional deve fornecer ferramentas para armazenar e reconfigurar as configurações do appliance a partir de arquivos de backup. A plataforma deve permitir que a MTU (unidade máxima de transmissão) seja customizada. Deve suportar os modos de Layer 2 (Transparente) e Layer 3 (roteamento). Deve suportar a criação de 4094 VLANs. Deve operar com IPv4 e IPv6, incluindo os protocolos de roteamento multicast. O sistema operacional deve suportar roteamento baseado em políticas, suportando a decisão de roteamento baseado em: • Endereço de origem • Comprimento da máscara de origem • Endereço de Destino • Comprimento da máscara de Destino Deve suportar NAT, incluindo: NAT64, NAT46, static NAT, dynamic NAT. Deve suportar protocolos de roteamento dinâmico (OSPFv2, RIPv2, BGP4). A plataforma deve suportar ao menos a conexão de 8 portas Gigabit virtuais criadas pelo hipervisor. O appliance deve suportar a utilização de funcionalidade de aceleração de tráfego para inspecionar o tráfego de rede com DPDK. O appliance deve possuir capacidade de armazenamento contingencial interno de pelo menos 60GB. REQUISITOS DE FUNCIONALIDADE FIREWALL O appliance deverá operar em Stateful Inspection baseado em análise do estado da comunicação e da aplicação para acompanhar e controlar o fluxo que passa por ele, desta forma, a solução deve ser capaz de: • Bloquear de pacotes fora de estado • Bloquear pacotes que desrespeitem um padrão estabelecido. Ex: um tráfego em cima de porta tcp 80 deve ser http, conforme estabelecido pelos órgãos reguladores. • Bloquear pacotes de sessões que atingiram um time-out pré-definido. • Liberar a resposta única e exclusivamente a uma solicitação de conexão previamente autorizada pelo Firewall. Ex: se tratando de TCP, somente permitir um SYN+ACK de um SYN já conhecido e autorizado. Deve suportar controle de acesso para pelo menos 60 aplicações/protocolos/serviços pré-definidos como: • http, https, ftp, ssh, smtp, domain-udp (DNS), domain-tcp, snmp, WINS, SIP, H323. Deve proteger a implementação de VoIP suportando H323 v2/3/4 (incluindo h.225 v2/3/4 e h.245 v3/5/7), SIP, MGCP e SCCP. Deve incluir NAT dinâmico (N-1 ou Hide) e estático (1-1), com a possibilidade de converter os IPs de origem e destino e as portas no mesmo pacote com apenas uma regra.

Item	Descrição
	Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP. Os seguintes esquemas de autenticação devem ser suportados pelos módulos de Firewall e VPN: Tokens (como SecurID), TACACS, RADIUS e certificados digitais. Deve ser capaz de trabalhar em Transparent mode (bridged mode). REQUISITOS DE FUNCIONALIDADE VPN O appliance deve permitir a autenticação entre peers VPN através de certificados do padrão PKCS#12, CAPI ou Entrust gerados por uma entidade interna da própria solução, ou uma externa. A comunicação entre o elemento de gerência e os firewalls deve ser autenticada através de certificados. Deve suportar criptografias 3DES e AES-256 para IKE fases I e II. Deve suportar pelo menos os seguintes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit) Deve suportar integridade de dados com md5 MD5, SHA256, SHA512 Deve incluir suporte para VPN site-to-site nas seguintes topologias: Full Meshed (todos para todos), Estrela (escritórios remotos para site central), Hub e Spoke (site remoto através de site central para outro site remoto). Deve incluir suporte a client-to-site baseado em IPsec. Deve suportar SSL-VPNs clientless, para acesso remoto sem necessidade de instalação de um agente. O cliente IPsec VPN incluso deve suportar auto-connect (uma conexão é feita automaticamente quando o endpoint está fora da rede corporativa e uma aplicação necessita acesso a essa rede), restabelecendo automaticamente caso haja qualquer falha ou mudança. Deve permitir que o administrador aplique regras de segurança para controlar o tráfego dentro da VPN. Deve permitir VPNs domain based ou policy-based e route-based. Deve incluir um mecanismo para mitigar o impacto de um ataque DoS ao IKE, fazendo a distinção entre peers conhecidos e desconhecidos. Deve incluir a funcionalidade para estabelecer VPNs com IPs públicos dinâmicos. O appliance deve ter certificação Common Criteria EAL4 para pelo menos os seguintes componentes: Firewall, VPN, IPS/ISD e Gateways de Acesso Remoto para IPsec e SSL. REQUISITOS DE FUNCIONALIDADE IPS O IPS integrado deve incluir pelo menos os seguintes mecanismos de detecção: Assinaturas de vulnerabilidades e exploits, assinaturas de Ataque, validação de Protocolo, detecção de anomalia, detecção baseada em comportamento, nível de confiança de detecção de ataque e correlação multi-elemento. O administrador deve ser capaz de configurar a inspeção somente para tráfego entrante (inbound). O IPS do UTM deve prover por padrão pelo menos um perfil pré-definido para ativação do produto sem necessidade de customização prévia por parte do administrador. Os dois perfis mínimos necessários devem possuir as seguintes características: • Política padrão: deve prover um baixo impacto computacional / alta performance enquanto provê um bom nível de proteção. • Política recomendada/mais segura: deve prover um alto nível de segurança e um bom nível de performance. A solução deve ser capaz de detectar e prevenir as seguintes ameaças: exploits e vulnerabilidades específicas de clientes e servidores, comunicação outbound de malware, tentativas de tunneling, controle de aplicações, ataques genéricos sem assinaturas pré-definidas. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na fonte, destino, serviço ou qualquer combinação dos três. A solução deve fazer captura de pacotes para proteções específicas. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações Web, Serviços de Email, DNS, FTP, serviços Windows (Microsoft Networking) e SNMP. Deve incluir a habilidade de detectar e bloquear tráfego peer to peer. A solução deve proteger contra o ataque DNS Cache Poisoning. Deve suportar e proteger os protocolos VoIP (H.323, SIP e SCCP).

Item	Descrição
	O administrador deve ser capaz de configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados. Deve-se permitir que o administrador bloqueie entrada e/ou saída de tráfego com base nos países, sem a necessidade de gerir manualmente os ranges de IP correspondentes a cada país. URL FILTERING URL Filtering baseado em categorias deve estar incluso como serviço. A solução deve cobrir mais de 20 milhões de URLs em pelo menos 40 categorias, incluindo: Adult, advertisements, chat, computing, criminal, drugs, education, finance, gambling, games, government, hacking, health, hosting sites, job search, news, personals & dating, reference, religion, remote proxies, search engines, sex education, shopping, social media, sports, streaming media, travel, violence, weapons. A solução deve incluir mecanismo de listas brancas e negras a fim de permitir aos administradores permitirem ou bloquear URLs específicas independente da categoria. A solução deve permitir exceções baseadas nos objetos de rede definidos. A solução deve oferecer a opção de modificar o aviso de bloqueio e redirecionar o usuário a outra página. REQUISITOS DE PERFORMANCE DO APPLIANCE O Firewall UTM com funcionalidade de IPS habilitada deverá possuir capacidade para manter um tráfego de 3 Gbps de throughput, sem degradar suas capacidades operacionais. Não serão aceitos números de performance expressos em UDP ou HTTP 1M. O Firewall UTM com IPsec VPN habilitada deverá possuir capacidade para manter 1,5 Gbps de throughput, sem degradar suas capacidades operacionais. O Firewall deve permitir que a funcionalidade de VPN inclua a licença necessária para, pelo menos, 5 usuários simultâneos utilizando a tecnologia SSL-VPN e 10 conexões simultâneas do tipo site-to-site utilizando a tecnologia IPsec. O appliance deve suportar pelo menos 30 mil conexões simultâneas ou “contextos de conexão”, sem degradar suas capacidades operacionais. O appliance deve ser capaz de atender a pelo menos 3 mil novas sessões por segundo, sem degradar suas capacidades operacionais. Os números de performance devem ser com a funcionalidade de aceleração DPDK desabilitada. GARANTIA O item ofertado em sua totalidade deve possuir garantia de 60 (sessenta) meses, a partir da data do aceite dos equipamentos. A proponente vencedora da licitação deverá entregar junto a todos os licenciamentos necessários para o cumprimento das exigências deste objeto, o termo de garantia. O período de disponibilidade para chamada dos serviços de manutenção dos equipamentos é de 24 horas por dia, 7 dias por semana.
02	Firewall UTM – Tipo 2 - VM4 O objeto aqui definido como “Firewall UTM” é também referenciado no mercado como Firewall de Última Geração – Next-Generation Firewall – (NGFW). Esses termos diversos poderão ser utilizados durante a descrição deste item, incluindo seus usos substanciados, como Firewall, UTM, NGFW, plataforma, equipamento ou mesmo appliance. Deverá estar licenciado para no mínimo 4 (quatro) vCPU cores. REQUISITOS GERAIS O Firewall UTM poderá ser instalado nas seguintes plataformas de virtualização: VMware ESXi (6.0) e KVM (versão disponível nos repositórios oficiais do CentOS 7). A imagem para instalação do appliance deverá ser fornecida em formato compatível com ambas as plataformas de virtualização. Deve possuir sistema operacional próprio preparado para atender serviços essenciais de segurança (Firewall, VPN, IPS). Este sistema operacional deve implementar uma interface gráfica web (usando http / https) que permite que todas as funções do sistema operacional e configurações tradicionais sejam realizadas, incluindo funções de troubleshooting. O Sistema Operacional do firewall deve ser capaz de adicionar novas funcionalidades sem a necessidade de reinstalação da solução. Os componentes da solução (incluindo o sistema operacional, drivers de dispositivos e aplicativos de segurança) devem ser desenvolvidos, produzidos e comercializados pela mesma fabricante. Deve implementar, diretamente no firewall ou na solução de gerenciamento centralizado a segmentação de acessos administrativos, permitindo que os administradores façam modificações

Item	Descrição
	nas configurações, relatórios e logs de maneira independente, sem que uma comprometa a outra. O sistema operacional do appliance deve suportar autenticação de usuários externa, através do protocolo RADIUS e/ou LDAP, e não deve exigir contas de usuário local a ser criado no sistema operacional, com exceção de um administrador para uso em caso de falha de comunicação com os servidores de autenticação externos. A solução deve ter integração com diretórios LDAP para autenticação e autorização de usuários baseado nos perfis armazenados no LDAP ou no firewall. Deve incluir a funcionalidade de pesquisar múltiplos servidores de LDAP para redundância e encontrar usuários distribuídos em múltiplos servidores de LDAP. O sistema operacional deve implementar política de senha de usuário administrador, com os seguintes requisitos: • Deve ser capaz de impor um tamanho mínimo e os diferentes tipos de caracteres (números, letras, caracteres especiais); • Deve ser capaz de forçar mudanças de senha periódica; • Deve acompanhar o histórico de senhas “velhas” para evitar a reutilização delas; • Deve implementar o bloqueio de conta de usuário depois de várias tentativas de login sem sucesso; • Deve implementar o bloqueio de conta de usuário após dias sem tentativas de login por longos períodos de tempo. A configuração do sistema operacional e monitoramento do mesmo deve suportar a administração baseada em perfis de acesso por grupo e/ou usuário. O sistema operacional deve suportar configurar um disclaimer (aviso legal) na tela de login do administrador do sistema operacional (NGFW). O sistema operacional deve suportar arquiteturas de clusters implementadas com balanceadores de carga (Load Balance). Deve suportar configurações de cluster e Alta Disponibilidade (High Availability - HA) que, em caso de falha de um dos nós do cluster, o impacto não seja perceptível para os utilizadores e as aplicações em modos ativo/standby e ativo/ativo na arquitetura implementada. O appliance deve suportar à gestão remota segura através da rede utilizando protocolo SSH e HTTPS, independente de software adicional. Suas interfaces de rede devem suportar VLANs (802.1Q e Trunking), assim como o tráfego non-tagged. Todos os componentes e processos críticos do sistema operacional devem gerar logs e suportar log remoto através do protocolo syslog, bem como utilizar o protocolo SNMP (versões 2 e 3), incluindo suporte traps de falhas e eventos. O sistema operacional deve possuir ferramenta de resolução de problemas em tempo real filtrando a captura de tráfego e armazenando-a, podendo exportá-la em formato compatível com a biblioteca libpcap. As configurações do sistema poderão ser exportadas como forma de backup sob demanda ou por agendamento para locais externos ao armazenamento do próprio appliance. O sistema operacional deve fornecer ferramentas para armazenar e reconfigurar as configurações do appliance a partir de arquivos de backup. A plataforma deve permitir que a MTU (unidade máxima de transmissão) seja customizada. Deve suportar os modos de Layer 2 (Transparente) e Layer 3 (roteamento). Deve suportar a criação de 4094 VLANs. Deve operar com IPv4 e IPv6, incluindo os protocolos de roteamento multicast. O sistema operacional deve suportar roteamento baseado em políticas, suportando a decisão de roteamento baseado em: • Endereço de origem • Comprimento da máscara de origem • Endereço de Destino • Comprimento da máscara de Destino Deve suportar NAT, incluindo: NAT64, NAT46, static NAT, dynamic NAT. Deve suportar protocolos de roteamento dinâmico (OSPFv2, RIPv2, BGP4). A plataforma deve suportar ao menos a conexão de 8 portas Gigabit virtuais criadas pelo hipervisor. O appliance deve suportar a utilização de funcionalidade de aceleração de tráfego para inspecionar

Item	Descrição
	o tráfego de rede com DPDK. O appliance deve possuir capacidade de armazenamento contingencial interno de pelo menos 60GB. REQUISITOS DE FUNCIONALIDADE FIREWALL O appliance deverá operar em Stateful Inspection baseado em análise do estado da comunicação e da aplicação para acompanhar e controlar o fluxo que passa por ele, desta forma, a solução deve ser capaz de: • Bloquear de pacotes fora de estado • Bloquear pacotes que desrespeitem um padrão estabelecido. Ex: um tráfego em cima de porta tcp 80 deve ser http, conforme estabelecido pelos órgãos reguladores. • Bloquear pacotes de sessões que atingiram um time-out pré-definido. • Liberar a resposta única e exclusivamente a uma solicitação de conexão previamente autorizada pelo Firewall. Ex: se tratando de TCP, somente permitir um SYN+ACK de um SYN já conhecido e autorizado. Deve suportar controle de acesso para pelo menos 60 aplicações/protocolos/serviços pré-definidos como: • http, https, ftp, ssh, smtp, domain-udp (DNS), domain-tcp, snmp, WINS, SIP, H323. Deve proteger a implementação de VoIP suportando H323 v2/3/4 (incluindo h.225 v2/3/4 e h.245 v3/5/7), SIP, MGCP e SCCP. Deve incluir NAT dinâmico (N-1 ou Hide) e estático (1-1), com a possibilidade de converter os IPs de origem e destino e as portas no mesmo pacote com apenas uma regra. Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP. Os seguintes esquemas de autenticação devem ser suportados pelos módulos de Firewall e VPN: Tokens (como SecurID), TACACS, RADIUS e certificados digitais. Deve ser capaz de trabalhar em Transparent mode (bridged mode). REQUISITOS DE FUNCIONALIDADE VPN O appliance deve permitir a autenticação entre peers VPN através de certificados do padrão PKCS#12, CAPI ou Entrust gerados por uma entidade interna da própria solução, ou uma externa. A comunicação entre o elemento de gerência e os firewalls deve ser autenticada através de certificados. Deve suportar criptografias 3DES e AES-256 para IKE fases I e II. Deve suportar pelo menos os seguintes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit) Deve suportar integridade de dados com md5 MD5, SHA256, SHA512 Deve incluir suporte para VPN site-to-site nas seguintes topologias: Full Meshed (todos para todos), Estrela (escritórios remotos para site central), Hub e Spoke (site remoto através de site central para outro site remoto). Deve incluir suporte a client-to-site baseado em IPsec. Deve suportar SSL-VPNs clientless, para acesso remoto sem necessidade de instalação de um agente. O cliente IPsec VPN incluso deve suportar auto-connect (uma conexão é feita automaticamente quando o endpoint está fora da rede corporativa e uma aplicação necessita acesso a essa rede), restabelecendo automaticamente caso haja qualquer falha ou mudança. Deve permitir que o administrador aplique regras de segurança para controlar o tráfego dentro da VPN. Deve permitir VPNs domain based ou policy-based e route-based. Deve incluir um mecanismo para mitigar o impacto de um ataque DoS ao IKE, fazendo a distinção entre peers conhecidos e desconhecidos. Deve incluir a funcionalidade para estabelecer VPNs com IPs públicos dinâmicos. O appliance deve ter certificação Common Criteria EAL4 para pelo menos os seguintes componentes: Firewall, VPN, IPS/ISD e Gateways de Acesso Remoto para IPsec e SSL. REQUISITOS DE FUNCIONALIDADE IPS O IPS integrado deve incluir pelo menos os seguintes mecanismos de detecção: Assinaturas de vulnerabilidades e exploits, assinaturas de Ataque, validação de Protocolo, detecção de anomalia, detecção baseada em comportamento, nível de confiança de detecção de ataque e correlação multi-elemento.

Item	Descrição
	O administrador deve ser capaz de configurar a inspeção somente para tráfego entrante (inbound). O IPS do UTM deve prover por padrão pelo menos um perfil pré-definido para ativação do produto sem necessidade de customização prévia por parte do administrador. Os dois perfis mínimos necessários devem possuir as seguintes características: • Política padrão: deve prover um baixo impacto computacional / alta performance enquanto provê um bom nível de proteção. • Política recomendada/mais segura: deve prover um alto nível de segurança e um bom nível de performance. A solução deve ser capaz de detectar e prevenir as seguintes ameaças: exploits e vulnerabilidades específicas de clientes e servidores, comunicação outbound de malware, tentativas de tunneling, controle de aplicações, ataques genéricos sem assinaturas pré-definidas. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na fonte, destino, serviço ou qualquer combinação dos três. A solução deve fazer captura de pacotes para proteções específicas. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações Web, Serviços de Email, DNS, FTP, serviços Windows (Microsoft Networking) e SNMP. Deve incluir a habilidade de detectar e bloquear tráfego peer to peer. A solução deve proteger contra o ataque DNS Cache Poisoning. Deve suportar e proteger os protocolos VoIP (H.323, SIP e SCCP). O administrador deve ser capaz de configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados. Deve-se permitir que o administrador bloqueie entrada e/ou saída de tráfego com base nos países, sem a necessidade de gerir manualmente os ranges de IP correspondentes a cada país. URL FILTERING URL Filtering baseado em categorias deve estar incluso como serviço. A solução deve cobrir mais de 20 milhões de URLs em pelo menos 40 categorias, incluindo: Adult, advertisements, chat, computing, criminal, drugs, education, finance, gambling, games, government, hacking, health, hosting sites, job search, news, personals & dating, reference, religion, remote proxies, search engines, sex education, shopping, social media, sports, streaming media, travel, violence, weapons. A solução deve incluir mecanismo de listas brancas e negras a fim de permitir aos administradores permitirem ou bloquear URLs específicas independente da categoria. A solução deve permitir exceções baseadas nos objetos de rede definidos. A solução deve oferecer a opção de modificar o aviso de bloqueio e redirecionar o usuário a outra página. REQUISITOS DE PERFORMANCE DO APPLIANCE O Firewall UTM com funcionalidade de IPS habilitada deverá possuir capacidade para manter um tráfego de 8 Gbps de throughput, sem degradar suas capacidades operacionais. Não serão aceitos números de performance expressos em UDP ou HTTP 1M. O Firewall UTM com IPsec VPN habilitada deverá possuir capacidade para manter 6 Gbps de throughput, sem degradar suas capacidades operacionais. O Firewall deve permitir que a funcionalidade de VPN inclua a licença necessária para, pelo menos, 5 usuários simultâneos utilizando a tecnologia SSL-VPN e 10 conexões simultâneas do tipo site-to-site utilizando a tecnologia IPsec. O appliance deve suportar pelo menos 60 mil conexões simultâneas ou “contextos de conexão”, sem degradar suas capacidades operacionais. O appliance deve ser capaz de atender a pelo menos 3 mil novas sessões por segundo, sem degradar suas capacidades operacionais. Os números de performance devem ser alcançados sem o uso da funcionalidade de aceleração DPDK. GARANTIA O item ofertado em sua totalidade deve possuir garantia de 60 (sessenta) meses, a partir da data do aceite dos equipamentos. A proponente vencedora da licitação deverá entregar junto a todos os licenciamentos necessários para o cumprimento das exigências deste objeto, o termo de garantia.

Item	Descrição
	O período de disponibilidade para chamada dos serviços de manutenção dos equipamentos é de 24 horas por dia, 7 dias por semana.
03	Firewall UTM – Tipo 3 - VM8 O objeto aqui definido como “Firewall UTM” é também referenciado no mercado como Firewall de Última Geração – Next-Generation Firewall – (NGFW). Esses termos diversos poderão ser utilizados durante a descrição deste item, incluindo seus usos substanciados, como Firewall, UTM, NGFW, plataforma, equipamento ou mesmo appliance. Deverá estar licenciado para no mínimo 8 (oito) vCPU cores. REQUISITOS GERAIS O Firewall UTM poderá ser instalado nas seguintes plataformas de virtualização: VMware ESXi (6.0) e KVM (versão disponível nos repositórios oficiais do CentOS 7). A imagem para instalação do appliance deverá ser fornecida em formato compatível com ambas as plataformas de virtualização. Deve possuir sistema operacional próprio preparado para atender serviços essenciais de segurança (Firewall, VPN, IPS). Este sistema operacional deve implementar uma interface gráfica web (usando http / https) que permite que todas as funções do sistema operacional e configurações tradicionais sejam realizadas, incluindo funções de troubleshooting. O Sistema Operacional do firewall deve ser capaz de adicionar novas funcionalidades sem a necessidade de reinstalação da solução. Os componentes da solução (incluindo o sistema operacional, drivers de dispositivos e aplicativos de segurança) devem ser desenvolvidos, produzidos e comercializados pela mesma fabricante. Deve implementar, diretamente no firewall ou na solução de gerenciamento centralizado a segmentação de acessos administrativos, permitindo que os administradores façam modificações nas configurações, relatórios e logs de maneira independente, sem que uma comprometa a outra. O sistema operacional do appliance deve suportar autenticação de usuários externa, através do protocolo RADIUS e/ou LDAP, e não deve exigir contas de usuário local a ser criado no sistema operacional, com exceção de um administrador para uso em caso de falha de comunicação com os servidores de autenticação externos. A solução deve ter integração com diretórios LDAP para autenticação e autorização de usuários baseado nos perfis armazenados no LDAP ou no firewall. Deve incluir a funcionalidade de pesquisar múltiplos servidores de LDAP para redundância e encontrar usuários distribuídos em múltiplos servidores de LDAP. O sistema operacional deve implementar política de senha de usuário administrador, com os seguintes requisitos: • Deve ser capaz de impor um tamanho mínimo e os diferentes tipos de caracteres (números, letras, caracteres especiais); • Deve ser capaz de forçar mudanças de senha periódica; • Deve acompanhar o histórico de senhas “velhas” para evitar a reutilização delas; • Deve implementar o bloqueio de conta de usuário depois de várias tentativas de login sem sucesso; • Deve implementar o bloqueio de conta de usuário após dias sem tentativas de login por longos períodos de tempo. A configuração do sistema operacional e monitoramento do mesmo deve suportar a administração baseada em perfis de acesso por grupo e/ou usuário. O sistema operacional deve suportar configurar um disclaimer (aviso legal) na tela de login do administrador do sistema operacional (NGFW). O sistema operacional deve suportar arquiteturas de clusters implementadas com balanceadores de carga (Load Balance). Deve suportar configurações de cluster e Alta Disponibilidade (High Availability - HA) que, em caso de falha de um dos nós do cluster, o impacto não seja perceptível para os utilizadores e as aplicações em modos ativo/standby e ativo/ativo na arquitetura implementada. O appliance deve suportar à gestão remota segura através da rede utilizando protocolo SSH e HTTPS, independente de software adicional. Suas interfaces de rede devem suportar VLANs (802.1Q e Trunking), assim como o tráfego non-tagged. Todos os componentes e processos críticos do sistema operacional devem gerar logs e suportar log remoto através do protocolo syslog, bem como utilizar o protocolo SNMP (versões 2 e 3), incluindo

Item	Descrição
	suporte traps de falhas e eventos. O sistema operacional deve possuir ferramenta de resolução de problemas em tempo real filtrando a captura de tráfego e armazenando-a, podendo exportá-la em formato compatível com a biblioteca libpcap. As configurações do sistema poderão ser exportadas como forma de backup sob demanda ou por agendamento para locais externos ao armazenamento do próprio appliance. O sistema operacional deve fornecer ferramentas para armazenar e reconfigurar as configurações do appliance a partir de arquivos de backup. A plataforma deve permitir que a MTU (unidade máxima de transmissão) seja customizada. Deve suportar os modos de Layer 2 (Transparente) e Layer 3 (roteamento). Deve suportar a criação de 4094 VLANs. Deve operar com IPv4 e IPv6, incluindo os protocolos de roteamento multicast. O sistema operacional deve suportar roteamento baseado em políticas, suportando a decisão de roteamento baseado em: • Endereço de origem • Comprimento da máscara de origem • Endereço de Destino • Comprimento da máscara de Destino Deve suportar NAT, incluindo: NAT64, NAT46, static NAT, dynamic NAT. Deve suportar protocolos de roteamento dinâmico (OSPFv2, RIPv2, BGP4). A plataforma deve suportar ao menos a conexão de 8 portas Gigabit virtuais criadas pelo hipervisor. O appliance deve suportar a utilização de funcionalidade de aceleração de tráfego para inspecionar o tráfego de rede com DPDK. O appliance deve possuir capacidade de armazenamento contingencial interno de pelo menos 60GB. REQUISITOS DE FUNCIONALIDADE FIREWALL O appliance deverá operar em Stateful Inspection baseado em análise do estado da comunicação e da aplicação para acompanhar e controlar o fluxo que passa por ele, desta forma, a solução deve ser capaz de: • Bloquear de pacotes fora de estado • Bloquear pacotes que desrespeitem um padrão estabelecido. Ex: um tráfego em cima de porta tcp 80 deve ser http, conforme estabelecido pelos órgãos reguladores. • Bloquear pacotes de sessões que atingiram um time-out pré-definido. • Liberar a resposta única e exclusivamente a uma solicitação de conexão previamente autorizada pelo Firewall. Ex: se tratando de TCP, somente permitir um SYN+ACK de um SYN já conhecido e autorizado. Deve suportar controle de acesso para pelo menos 60 aplicações/protocolos/serviços pré-definidos como: • http, https, ftp, ssh, smtp, domain-udp (DNS), domain-tcp, snmp, WINS, SIP, H323. Deve proteger a implementação de VoIP suportando H323 v2/3/4 (incluindo h.225 v2/3/4 e h.245 v3/5/7), SIP, MGCP e SCCP. Deve incluir NAT dinâmico (N-1 ou Hide) e estático (1-1), com a possibilidade de converter os IPs de origem e destino e as portas no mesmo pacote com apenas uma regra. Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP. Os seguintes esquemas de autenticação devem ser suportados pelos módulos de Firewall e VPN: Tokens (como SecurID), TACACS, RADIUS e certificados digitais. Deve ser capaz de trabalhar em Transparent mode (bridged mode). REQUISITOS DE FUNCIONALIDADE VPN O appliance deve permitir a autenticação entre peers VPN através de certificados do padrão PKCS#12, CAPI ou Entrust gerados por uma entidade interna da própria solução, ou uma externa. A comunicação entre o elemento de gerência e os firewalls deve ser autenticada através de certificados. Deve suportar criptografias 3DES e AES-256 para IKE fases I e II. Deve suportar pelo menos os seguintes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit) Deve suportar integridade de dados com md5 MD5, SHA256, SHA512

Item	Descrição
	Deve incluir suporte para VPN site-to-site nas seguintes topologias: Full Meshed (todos para todos), Estrela (escritórios remotos para site central), Hub e Spoke (site remoto através de site central para outro site remoto). Deve incluir suporte a client-to-site baseado em IPsec. Deve suportar SSL-VPNs clientless, para acesso remoto sem necessidade de instalação de um agente. O cliente IPsec VPN incluso deve suportar auto-connect (uma conexão é feita automaticamente quando o endpoint está fora da rede corporativa e uma aplicação necessita acesso a essa rede), restabelecendo automaticamente caso haja qualquer falha ou mudança. Deve permitir que o administrador aplique regras de segurança para controlar o tráfego dentro da VPN. Deve permitir VPNs domain based ou policy-based e route-based. Deve incluir um mecanismo para mitigar o impacto de um ataque DoS ao IKE, fazendo a distinção entre peers conhecidos e desconhecidos. Deve incluir a funcionalidade para estabelecer VPNs com IPs públicos dinâmicos. O appliance deve ter certificação Common Criteria EAL4 para pelo menos os seguintes componentes: Firewall, VPN, IPS/ISD e Gateways de Acesso Remoto para IPsec e SSL. REQUISITOS DE FUNCIONALIDADE IPS O IPS integrado deve incluir pelo menos os seguintes mecanismos de detecção: Assinaturas de vulnerabilidades e exploits, assinaturas de Ataque, validação de Protocolo, detecção de anomalia, detecção baseada em comportamento, nível de confiança de detecção de ataque e correlação multi-elemento. O administrador deve ser capaz de configurar a inspeção somente para tráfego entrante (inbound). O IPS do UTM deve prover por padrão pelo menos um perfil pré-definido para ativação do produto sem necessidade de customização prévia por parte do administrador. Os dois perfis mínimos necessários devem possuir as seguintes características: • Política padrão: deve prover um baixo impacto computacional / alta performance enquanto provê um bom nível de proteção. • Política recomendada/mais segura: deve prover um alto nível de segurança e um bom nível de performance. A solução deve ser capaz de detectar e prevenir as seguintes ameaças: exploits e vulnerabilidades específicas de clientes e servidores, comunicação outbound de malware, tentativas de tunneling, controle de aplicações, ataques genéricos sem assinaturas pré-definidas. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na fonte, destino, serviço ou qualquer combinação dos três. A solução deve fazer captura de pacotes para proteções específicas. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações Web, Serviços de Email, DNS, FTP, serviços Windows (Microsoft Networking) e SNMP. Deve incluir a habilidade de detectar e bloquear tráfego peer to peer. A solução deve proteger contra o ataque DNS Cache Poisoning. Deve suportar e proteger os protocolos VoIP (H.323, SIP e SCCP). O administrador deve ser capaz de configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados. Deve-se permitir que o administrador bloqueie entrada e/ou saída de tráfego com base nos países, sem a necessidade de gerir manualmente os ranges de IP correspondentes a cada país. URL FILTERING URL Filtering baseado em categorias deve estar incluso como serviço. A solução deve cobrir mais de 20 milhões de URLs em pelo menos 40 categorias, incluindo: Adult, advertisements, chat, computing, criminal, drugs, education, finance, gambling, games, government, hacking, health, hosting sites, job search, news, personals & dating, reference, religion, remote proxies, search engines, sex education, shopping, social media, sports, streaming media, travel, violence, weapons. A solução deve incluir mecanismo de listas brancas e negras a fim de permitir aos administradores permitirem ou bloquear URLs específicas independente da categoria. A solução deve permitir exceções baseadas nos objetos de rede definidos.

Item	Descrição
	A solução deve oferecer a opção de modificar o aviso de bloqueio e redirecionar o usuário a outra página. REQUISITOS DE PERFORMANCE DO APPLIANCE O Firewall UTM com funcionalidade de IPS habilitada deverá possuir capacidade para manter um tráfego de 8 Gbps de throughput, sem degradar suas capacidades operacionais. Não serão aceitos números de performance expressos em UDP ou HTTP 1M. O Firewall UTM com IPsec VPN habilitada deverá possuir capacidade para manter 6 Gbps de throughput, sem degradar suas capacidades operacionais. O Firewall deve permitir que a funcionalidade de VPN inclua a licença necessária para, pelo menos, 5 usuários simultâneos utilizando a tecnologia SSL-VPN e 10 conexões simultâneas do tipo site-to-site utilizando a tecnologia IPsec. O appliance deve suportar pelo menos 60 mil conexões simultâneas ou “contextos de conexão”, sem degradar suas capacidades operacionais. O appliance deve ser capaz de atender a pelo menos 3 mil novas sessões por segundo, sem degradar suas capacidades operacionais. Os números de performance devem ser alcançados sem o uso da funcionalidade de aceleração DPDK. GARANTIA O item ofertado em sua totalidade deve possuir garantia de 60 (sessenta) meses, a partir da data do aceite dos equipamentos. A proponente vencedora da licitação deverá entregar junto a todos os licenciamentos necessários para o cumprimento das exigências deste objeto, o termo de garantia. O período de disponibilidade para chamada dos serviços de manutenção dos equipamentos é de 24 horas por dia, 7 dias por semana.
04	Solução para Gerenciamento das unidades de Firewall UTM O objeto aqui definido como “Solução para Gerenciamento das unidades de Firewall UTM” deverá ser compatível com os itens 1,2 e 3 deste Termo de Referência. A solução poderá ser dividida em até duas máquinas virtuais, operando funções distintas, mas que atendam ao descrito neste objeto. Considerar os mesmos termos para “Firewall UTM” adotados nos Itens 1,2 e 3 Requisitos básicos: • A solução deve permitir cadastrar todos os Firewalls do Órgão equivalentes aos itens 1 e 2 deste Termo de Referência. • A solução deve incluir a opção de gerenciamento central de interfaces de Firewalls, rotas, DNS e outros parâmetros desde uma console gráfica. • A solução deve incluir a habilidade de enviar e executar scripts em alguns ou todos os Firewalls gerenciados cadastrados ao mesmo tempo a partir de uma console gráfica central. • A solução deve incluir a opção de agendamento centralizado de backups para alguns ou todos os Firewalls gerenciados e executar centralmente backups sob demanda a partir de uma console gráfica. • A solução deve permitir armazenar seus registros de dados coletados em equipamento(s) externo(s). • As configurações do sistema poderão ser exportadas como forma de backup sob demanda ou por agendamento para locais externos ao armazenamento do próprio appliance. • O sistema operacional deve fornecer ferramentas para armazenar e reconfigurar as configurações do appliance a partir de arquivos de backup. • A solução deve permitir e estar licenciada para armazenamento de logs maior ou igual a 10TB. MONITORAMENTO A solução deve incluir uma interface de monitoramento gráfico pré-configurada e customizável que forneça formas para monitorar os status dos Firewalls cadastrados, incluindo: • Versão do Sistema Operacional, consumo de CPU, consumo de memória, % de HD livre, atividade de rede, números de sessões simultâneas e número de sessões novas abertas por segundo. • A comunicação entre a solução de gerenciamento e os firewalls deve ser criptografada e autenticada.

Item	Descrição
	• A solução deve informar o status de cada componente do UTM (Ex.: Firewall, VPN, IPS, entre outros). • A solução deve informar o status de todos os túneis de VPN, site-to-site e client-to-site. A solução deve incluir um limite configurável que, quando atingido, deve iniciar uma determinada ação (ou ações). As ações devem incluir: • Log, alerta, envio de um SNMP trap, envio de email e execução de um script definido pelo usuário. • Deve incluir a opção de reiniciar um túnel VPN para desconectar um usuário remoto da interface gráfica. • A solução deve ser capaz, de maneira dinâmica, através de regras de controle, bloquear temporariamente pacotes baseado na fonte, destino ou serviço. • A solução deve ser capaz de monitorar perda de pacotes, uso de banda e atrasos entre dois pontos conectados por uma VPN, logs e alertas quando um túnel de VPN estiver down. GARANTIA O item ofertado em sua totalidade deve possuir garantia de 60 (sessenta) meses, a partir da data do aceite dos equipamentos. A proponente vencedora da licitação deverá entregar junto a todos os licenciamentos necessários para o cumprimento das exigências deste objeto, o termo de garantia. O período de disponibilidade para chamada dos serviços de manutenção dos equipamentos é de 24 horas por dia, 7 dias por semana.
05	Software de coleta e análise de logs centralizado Deve estar incluída uma ferramenta para gerenciamento de eventos de IPS. Deve permitir a criação de filtros com base em qualquer característica de evento IPS, tais como a origem e o destino IP, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, entre outros. O administrador deve ser capaz de atribuir aos filtros gráficos de linhas diferentes, que são atualizadas em intervalos regulares, mostrando todos os eventos que correspondam a esse filtro, permitindo ao operador concentrar-se sobre os acontecimentos mais importantes na sua rede. A lista de eventos deve incluir a opção de gerar automaticamente pequenos gráficos ou tabelas com o evento, a origem e o destino de distribuição. Deve incluir uma ferramenta para correlacionar eventos de todos os recursos do appliance; Deve detectar ataques de negação de serviço e correlacionar eventos de todas as fontes; Deve detectar um login dos administradores irregulares; Deve detectar ataques de adivinhação de credencial; A ferramenta de relatórios deve suportar pelo menos 25 filtros (por exemplo, origem, destino, usuário, nome do ataque e número da regra), que permita personalizar um relatório (pré-definidos) para ser o mais próximo das necessidades do administrador (Ex.: atividade na web de um usuário específico); Deve suportar a programação de relatórios automáticos agendados pelo administrador para as informações básicas que precisa extrair de forma diária, semanal e mensal; Ele deve suportar os seguintes formatos de relatórios: HTML, CSV e PDF; A ferramenta de relatórios deve fornecer informações consolidadas sobre: • O volume de ligações que foram bloqueadas pelo ponto de aplicação (perímetro) • Top fontes de conexões bloqueadas, seus destinos e serviços; • Regras Top usado pelo ponto de aplicação (perímetro); • Top ataques à segurança detectadas pelo ponto de aplicação (perímetro) a determinação das suas principais fontes e os destinos; • Número de políticas instalada e desinstalada no ponto de aplicação; • Top serviços de rede; • Atividades Web sobre os sites mais visitados e usuários top web; • Atividades SMTP sobre os top remetentes de correio e seus top receptores beneficiários; • Atividade de FTP detalhando o top usuários e top arquivos de FTP (upload / download); • Top serviços, que utilizou mais tráfego criptografado; • Top usuários VPN realizar a maiores durações conexões;

Item	Descrição
	GARANTIA O item ofertado em sua totalidade deve possuir garantia de 60 (sessenta) meses, a partir da data do aceite dos equipamentos. A proponente vencedora da licitação deverá entregar junto a todos os licenciamentos necessários para o cumprimento das exigências deste objeto, o termo de garantia. O período de disponibilidade para chamada dos serviços de manutenção dos equipamentos é de 24 horas por dia, 7 dias por semana.
06	INSTALAÇÃO E CONFIGURAÇÃO A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes, em prazo máximo de 30 (trinta) dias após a oficialização da ordem de empenho. O planejamento anterior ao serviço pode ser realizado remotamente através de videoconferência. O Órgão deverá comunicar à CONTRATADA suas necessidades que poderão ser ajustadas durante a prestação do serviço, não ultrapassando 1 mês após a primeira reunião de planejamento. Ao fim da prestação do serviço, a CONTRATADA deverá enviar a documentação final contendo um relatório detalhado com todos os itens configurados no projeto (as-built), devendo também incluir toda informação pertinente à posterior continuidade e manutenção da solução instalada. Esta documentação deverá ser assinada pela equipe técnica da CONTRATADA pelo fiscal técnico do contrato, validando-a. TREINAMENTO DA SOLUÇÃO Realização de treinamento aos analistas e técnicos de TI do Órgão em que estiverem instalados os itens 1, 2 e 3 deste Termo de Referência. Esse treinamento poderá ser dividido em até duas turmas de até 10 pessoas cada turma com carga horária mínima de 20h, podendo ocorrer nas modalidades EAD, presencial ou híbrida, sendo ministrado por pessoa(s) certificada(s) pelo fabricante. O conteúdo deve abordar as funcionalidades básicas e as funcionalidades implementadas e/ou planejadas para implementação no Órgão, além de também abordar funcionalidades de personalização para emissão de relatórios. Após a finalização do treinamento, a CONTRATADA, deverá emitir certificado individual de conclusão, para todos os participantes. O certificado de conclusão deverá ser emitido em português brasileiro. APOIO TÉCNICO ESPECIALIZADO SOB DEMANDA A CONTRATADA deverá disponibilizar no mínimo 1 (um) Especialista para fornecer apoio técnico especializado para implementação de novas tecnologias, integrações, adoção e otimização de soluções, alterações de topologia, criação de regras e políticas, movimentações entre outros; A CONTRATANTE deverá solicitar a CONTRATADA o agendamento do atendimento que deverá ser oferecido sempre em duas opções de data pela CONTRATADA; A CONTRATANTE deverá abrir um chamado na CONTRATADA informando o escopo pretendido, a CONTRATADA irá apresentar uma ordem de serviço e termo de aceite com a estimativa de horas a serem utilizadas, a CONTRATANTE assina o termo de aceite, logo a CONTRATADA executa os serviços. Os tópicos a serem abordados deverão ser informados durante o agendamento; O Especialista será responsável apenas por tecnologias relacionadas aos equipamentos e softwares dos serviços contratados; O Especialista será pode auxiliar no planejamento, além de apoiar, orientar e acompanhar conforme solicitação da CONTRATANTE; O apoio técnico especializado sob demanda tem por finalidade mitigar não só os potenciais riscos quanto à possível indisponibilidade de sistema, mas como viabilizar melhor aproveitamento de experiência da solução e suas funcionalidades, incluindo a configuração de regras, instalação, auxílio em backup e atualização da solução ofertada por parte da CONTRATADA. Esse serviço deverá ser realizado de forma local ou remota para assegurar que as operações diárias sejam realizadas normalmente, conforme a necessidade, e contemplar, pelo menos, as seguintes atividades: • A CONTRATADA deverá observar as melhores práticas de mercado para ambientes similares de forma a se obter uma uniformidade nos controles e padrões de segurança. O Especialista poderá executar as seguintes atividades: · Configuração, atualizações e ajustes na plataforma, aplicação de melhores práticas do fabricante; · Elaboração de parecer em segurança da informação;

Item	Descrição
	· Apresentações de novos versionamentos da solução, indicando as funcionalidades, ganhos, riscos e impactos ao ambiente. • Auxílio na criação de regras e políticas; • Criação e revisão de plano de configuração; • Criação e revisão de plano de testes; • Criação e revisão de plano de implementação; • Criação e revisão de desenho/arquitetura; • Criação e revisão de plano de contingência; • Criação e revisão de plano de mudanças; • Adotar sempre as melhores práticas do mercado; • Apoio na execução de atualizações; • Análise de logs de equipamentos; • Discussão de novas tecnologias; • Apontamento de cenários diversos; • Dúvidas e sugestões; A CONTRATADA deverá observar as melhores práticas de mercado para ambientes similares de forma a se obter uma uniformidade nos controles e padrões de segurança. Configuração do equipamento ou software sobre os seguintes aspectos: • Definição da rede de gerência. • Conectividade com todos os dispositivos de rede. • Definição da rede e seus parâmetros de conectividades. • Definição de roteamento IP na rede. Será de responsabilidade da CONTRATANTE toda e qualquer intervenção física e lógica nos equipamentos e softwares; O total de horas a serem disponibilizadas é de 100 (cem) horas por semestre; As horas contratadas não utilizadas não serão acumulativas para o próximo semestre de contrato; O especialista disponibilizado pela contratada deverá atender no mínimo as seguintes qualificações: • 5 (cinco) anos de experiência em implementação, configuração e resolução de problemas/suporte nos equipamentos e soluções objetos do contrato; • Certificação de nível profissional do fabricante ofertado; • Curso superior em Tecnologia da Informação ou curso superior em qualquer área de formação com pós-graduação na área de tecnologia da informação; Caso solicitado, a CONTRATADA deverá enviar as comprovações técnicas assim como comprovação de vínculo empregatício ou contrato de prestação de serviço do profissional especialista em prazo de até 30 (trinta) dias após a assinatura do contrato;
07	Autodesk AutoCAD LT Software de CAD (projeto auxiliado por computador) usado para esboços 2D, projetos e documentação precisos. Inclui recursos para automatizar tarefas e aumentar a produtividade, como comparação de desenhos, contagem, adição de objetos e criação de tabelas. Permite criar, editar e anotar desenhos por meio de desktop, Web e dispositivos móveis por um período de 36 (trinta e seis) meses.
08	Autodesk Architecture, Engineering & Construction Collection (AEC Collection) Pacote de softwares de CAD e BIM, incluindo AutoCAD, Revit, Autodesk Forma, InRoads, Civil 3D, Autodesk Docs, entre outros, bem como um ambiente de dados comum com base na nuvem, permitindo que projetistas, engenheiros e contratados entreguem com eficiência projetos de construção e infraestrutura. As avançadas ferramentas de projeto conceitual ajudam os profissionais de AEC a realizar a ideia do projeto, enquanto as soluções de projeto baseadas em modelos aceleram os processos de projeto e dão suporte a fluxos de trabalho integrados para coordenação multidisciplinar. As ferramentas de análise e otimização melhoram a qualidade do projeto e garantem a viabilidade da construção por um período de 36 (trinta e seis) meses.

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio:

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

A solução de proteção de rede deverá atender aos seguintes requisitos de negócio do IFSertãoPE:

- **RN01 — Segurança da Infraestrutura Institucional:** Garantir a proteção da infraestrutura de rede institucional contra ameaças cibernéticas, incluindo ataques externos, tentativas de intrusão e tráfego malicioso.
- **RN02 — Continuidade dos Serviços de TI :**Assegurar a disponibilidade e continuidade dos serviços digitais institucionais, reduzindo riscos de indisponibilidade causados por incidentes de segurança.
- **RN03 — Proteção de Dados Institucionais:** Contribuir para a proteção de dados institucionais e informações sensíveis armazenadas e trafegadas na rede corporativa.
- **RN04 — Monitoramento e Visibilidade da Rede:** Permitir monitoramento contínuo do tráfego de rede e geração de registros (logs) que possibilitem auditoria, rastreabilidade e análise de incidentes de segurança.
- **RN05 — Gestão Centralizada de Segurança:** Disponibilizar mecanismos que permitam gerenciamento centralizado das políticas de segurança da rede institucional.
- **RN06 — Conformidade com Normas de Segurança:** Atender às diretrizes e políticas de segurança da informação adotadas pela instituição e às recomendações de boas práticas de segurança cibernética.
- **RN07 — Escalabilidade e Evolução Tecnológica:** emitir evolução da solução de segurança, acompanhando o crescimento da infraestrutura de TIC e o aumento do tráfego de rede.
- **RN08 — Apoio à Governança de TIC:** Disponibilizar recursos que auxiliem na gestão, auditoria e governança dos ambientes de rede e segurança da informação.

A solução de softwares de engenharia deverá atender aos seguintes requisitos de negócio do IFSertãoPE:

- **RN09 — Suporte às Atividades de Engenharia e Arquitetura:** Disponibilizar ferramentas tecnológicas adequadas para elaboração de projetos de engenharia, arquitetura e infraestrutura
- **RN10 — Apoio à Elaboração de Projetos Institucionais:** Permitir a criação, edição e gestão de projetos técnicos relacionados a obras, infraestrutura e planejamento institucional.
- **RN11 — Compatibilidade com Padrões de Engenharia:** Disponibilizar softwares amplamente utilizados no mercado e compatíveis com padrões técnicos adotados em projetos de engenharia e arquitetura.
- **RN12 — Apoio ao Ensino, Pesquisa e Extensão:** Contribuir para o desenvolvimento de atividades acadêmicas, científicas e tecnológicas nas áreas de engenharia e arquitetura
- **RN13 — Integração entre Ferramentas de Projeto:** Possibilitar a integração entre diferentes ferramentas utilizadas na elaboração e modelagem de projetos técnicos.
- **RN14 — Atualização Tecnológica:** Garantir acesso a versões atualizadas das ferramentas utilizadas nos processos de elaboração de projetos técnicos.

- **RN15 — Conformidade com Metodologias Modernas de Projeto:** Disponibilizar ferramentas que permitam utilização de metodologias modernas de desenvolvimento de projetos, como modelagem BIM.

Requisitos de Capacitação

- 4.2. Deverão ser realizadas reuniões de ponto de controle, sob demanda, para solução de dúvidas sobre a gestão o ambiente entre a CONTRATADA e o IF Sertão PE.
- 4.3. A CONTRATADA deverá prover, sempre que necessário, capacitação da ferramenta utilizada para gestão de demandas aos servidores responsáveis pela gestão do contrato, para possibilitar o monitoramento do trabalho executado pela CONTRATADA.

Requisitos Legais

- 4.4. 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

- 4.5. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e a outras legislações aplicáveis;
- 4.6. A CONTRATADA deverá observar os critérios de sustentabilidade ambiental descrito no Decreto nº 7.404, de 23 de dezembro de 2010, na IN/SLTI/MP nº 1, de 19 de janeiro de 2010, e no Decreto nº 7.746, de 5 de junho de 2012.

Requisitos Temporais

- 4.7. Os serviços devem ser prestados no prazo máximo de **15 (quinze) dias corridos**, 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;
- 4.8. 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.
- 4.9. 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.
- 4.10. Na execução dos serviços, deverão ser observados os seguintes prazos:

Atividade, Tarefa ou Serviço	Prazo máximo de início de atendimento	Prazo máximo de solução de problema
Disponibilização das licenças das soluções NGFW e Autodesk	até 5 dias úteis	até 5 dias úteis
Ativação e validação das licenças	até 4 horas	até 4 horas
Atendimento a solicitações de suporte técnico ou esclarecimentos	até 24 horas	até 3 dias úteis

Requisitos de Segurança e Privacidade

4.10.1 A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do CONTRATANTE, e os profissionais envolvidos na sua operacionalização deverão atender plenamente às seguintes condições:

- Requisitos de segurança e procedimentos definidos para o acesso às dependências do IFSertãoPE, bem como requisitos de segurança da informação e de vedação de acesso e divulgação, conforme se aplique, a informações classificadas e privadas, bem como a informações privilegiadas, isto é, aquelas que por qualquer motivo possam vir a representar vantagem mercantil competitiva;
- Sigilo sobre iniciativas, projetos, decisões, dados e qualquer outro tipo de informação de que venham a ter conhecimento durante a execução dos serviços, não podendo divulgá-las ou utilizá-las, durante a execução dos serviços e mesmo após seu encerramento, sem a expressa autorização do IFSertãoPE.

Deverão ser observados os requisitos de Segurança da Informação e Privacidade (SIP) de dados pessoais, nos termos definidos nas demais seções deste TR, bem como possíveis exigências ulteriores, baseados no "Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade" publicado pela SGD /ME (https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-dados/guias/guia_requisitos_obrigacoes.pdf/view), e suas eventuais atualizações, tendo em conta os princípios da razoabilidade e interesse público.

Requisitos Sociais, Ambientais e Culturais

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

- No que couber, visando a atender ao disposto na legislação aplicável – em destaque às Instruções Normativas 05/2017/SEGES e 01/2019/SGD – a CONTRATADA deverá priorizar, para a execução dos serviços, a utilização de bens que sejam no todo ou em partes compostos por materiais recicláveis, atóxicos e biodegradáveis.
- Ainda, no que se refere aos requisitos de sustentabilidade ambiental, a empresa CONTRATADA deverá garantir, no que couber, o descarte correto e seguro de todos os insumos/itens que forem removidos em manutenções, adotando práticas de sustentabilidade ambiental na execução do objeto. Deverá adotar medidas, quando couber, para atender as recomendações contidas no Capítulo III, DOS BENS E SERVIÇOS, com ênfase no art. 6º da Instrução Normativa nº 01/2010 SLTI/MPOG, bem como, o Decreto nº 7.746/2012 que estabelece critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável e a Lei nº 12.305/2010 que institui a política de resíduos sólidos.

- A empresa CONTRATADA deverá contribuir para a promoção do desenvolvimento nacional sustentável no cumprimento de diretrizes e critérios de sustentabilidade ambiental de acordo com o art. 225 da Constituição Federal de 1988, em conformidade com o art. 3º da Lei nº 14.133/21.
- A presente contratação deverá prezar, sempre que possível, por documentos em meios digitais em detrimento ao uso de papel impresso.
- O acesso aos serviços deverá estar disponível no idioma português do Brasil.

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.

4.14. As especificações técnicas e demais requisitos da solução estão detalhadas no TR.

Requisitos de Projeto e de Implementação

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

- A CONTRATANTE deverá manter uma equipe técnica responsável por acompanhar a execução do contrato, cobrando da CONTRATADA os prazos determinados para fornecimento dos itens licitados, instalação das licenças, instalação da solução de segurança e execução dos repasses de conhecimento. Ao final da execução do contrato, a CONTRATADA deverá fornecer a documentação de todos os trabalhos realizados no IFSertãoPE.
- A CONTRATADA deverá disponibilizar profissional técnico responsável pelo acompanhamento da implantação da solução no IFSertãoPE, a fim de tratar das questões técnicas e administrativas.
- O recebimento dos itens licitados se dará:
 - Provisório, no prazo máximo de 15 (quinze) dias, contados da efetiva entrega no IFSertãoPE para posterior verificação da conformidade das licenças e certificados de garantia com as especificações, constando das seguintes fases:
 - Instalação das licenças;
 - Comprovação de que as licenças fornecidas atendem às especificações mínimas exigidas ou aquelas superiores oferecidas;
 - Comprovação de que os certificados de garantia atendem às especificações mínimas exigidas;
 - Transferência de conhecimento aos técnicos da CONTRATANTE;
 - Definitivo, no prazo máximo de 15 (quinze) dias corridos contados a partir do recebimento provisório e após a verificação da qualidade dos objetos contratados e sua consequente aceitação, mediante a emissão do Termo de Recebimento Definitivo assinado pelas partes.
- O recebimento provisório dos itens licitados não constitui aceitação deles. Se, após o recebimento provisório, constatar-se que alguns dos itens foi entregue em desacordo com o solicitado, fora da especificação ou incompleto, a CONTRATADA será notificada e estará sujeita a aplicação de sanções cabíveis.

Requisitos de Implantação

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

- **RI01 – Disponibilização das licenças:** A contratada deverá fornecer e disponibilizar as licenças das soluções NGFW e Autodesk AEC Collection, devidamente registradas junto ao fabricante.
- **RI02 – Ativação das soluções:** A contratada deverá realizar a ativação das licenças e garantir o acesso às funcionalidades contratadas.
- **RI03 – Configuração da solução de segurança:** Para a solução NGFW, a contratada deverá realizar a instalação e configuração inicial da solução, incluindo integração com a infraestrutura de rede da Contratante.
- **RI04 – Acesso às ferramentas Autodesk:** A contratada deverá disponibilizar acesso às ferramentas do pacote Autodesk AEC Collection por meio do portal do fabricante.
- **RI05 – Testes de funcionamento:** Após a implantação, deverão ser realizados testes para verificação do funcionamento adequado das soluções.
- **RI06 – Transferência de conhecimento:** A contratada deverá realizar repasse de conhecimento à equipe técnica da Contratante quanto à operação e administração da solução NGFW.
- **RI07 – Aceite da implantação:** A implantação será considerada concluída após validação técnica da contratante quanto ao correto funcionamento das soluções.

Requisitos de Garantia e Manutenção

4.17. O prazo de garantia é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e suas atualizações.

A solução deverá atender aos seguintes requisitos de garantia e manutenção durante todo o período de vigência contratual:

- **RGM01 – Garantia das licenças:** As licenças das soluções deverão possuir garantia e suporte do fabricante durante todo o período contratado.
- **RGM02 – Atualizações e correções:** A contratada deverá garantir acesso às atualizações de versão, correções de falhas e atualizações de segurança disponibilizadas pelo fabricante.
- **RGM03 – Suporte técnico:** A contratada deverá disponibilizar suporte técnico para atendimento de incidentes, falhas ou dúvidas relacionadas às soluções fornecidas.
- **RGM04 – Correção de falhas:** A contratada deverá atuar na identificação e correção de falhas ou inconsistências que comprometam o funcionamento das soluções.
- **RGM05 – Manutenção evolutiva:** As soluções deverão permitir atualização tecnológica durante o período contratual, conforme disponibilizado pelo fabricante.

Requisitos de Experiência Profissional

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

Requisitos de Formação da Equipe

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

- A CONTRATADA é responsável pelos profissionais que atuarão na instalação dos equipamentos e manutenção (caso seja necessário), bem como por sua capacitação/especialização, assumindo assim toda responsabilidade pelos trabalhos realizados por sua equipe técnica.

Requisitos de Metodologia de Trabalho

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

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

4.22. O CONTRATADO deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana de maneira eletrônica e 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana por via telefônica ou ferramenta de comunicação instantânea.

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

Requisitos de Segurança da Informação e Privacidade

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

- A CONTRATADA deverá respeitar as diretrizes constantes da Política de Segurança da Informação (POSIN) do IFSertãoPE em vigência;
- Os serviços contratados deverão ser executados em conformidade com leis, normas e diretrizes do Governo relacionadas à Segurança da Informação e Comunicações (SIC), em especial ao Decreto 9.637, de 26 de dezembro de 2018 e normas complementares;
- A CONTRATADA deverá tomar todas as providências necessárias para que seus funcionários observem os regulamentos, normas, instruções de segurança, políticas de informação e comunicações adotados pelo Ministério do Turismo, inclusive normas internas de segurança, além de firmar Termo de Compromisso e Confidencialidade. Além disso, os funcionários responsáveis pela execução do contrato deverão assinar Termo de Ciência;

A CONTRATADA deverá apresentar, na reunião inicial, relação nominal dos profissionais envolvidos na execução do contrato que deverão ter acesso às instalações do IFSertãoPE. Caberá ao preposto manter esta lista atualizada sempre que um novo profissional necessitar de acesso ao IFSertãoPE. A lista deverá conter nome completo, número de identidade, CPF e data de início de atuação na prestação dos serviços (e de término, quando este não estiver mais alocado ao contrato).

Vistoria

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

Sustentabilidade

4.26. 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:

- A CONTRATADA deverá garantir a conformidade com a Lei nº 12.305/2010 que instituiu a Política Nacional de Resíduos Sólidos.

Indicação de marcas ou modelos

4.27. 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.

a) Solução de Segurança de Rede – Next Generation Firewall (NGFW)

Para o grupo referente à solução de segurança de rede, será admitida a indicação da marca **Fortinet**, especificamente da linha **FortiGate**, incluindo os componentes de gerenciamento e análise associados.

Tal indicação justifica-se pelo fato de que o Instituto Federal do Sertão Pernambucano já utiliza a plataforma Fortinet FortiGate como solução padrão de segurança perimetral, estando implantada em todos os campi e na Reitoria, com integração entre os dispositivos e demais ferramentas de monitoramento e gestão da infraestrutura de rede.

A continuidade da utilização dessa plataforma permite:

- manutenção da compatibilidade com a infraestrutura de segurança existente;
- aproveitamento dos equipamentos e do ambiente já implantado;
- preservação do conhecimento técnico já consolidado pela equipe de Tecnologia da Informação;
- redução de custos e riscos associados à migração para outra solução;
- garantia de integração com os demais componentes da arquitetura de segurança institucional.

Dessa forma, a adoção da solução Fortinet/FortiGate mostra-se tecnicamente mais adequada e economicamente vantajosa para a instituição.

b) Solução de Software CAD

Para o grupo referente aos softwares de desenho técnico e engenharia, será admitida a indicação da marca Autodesk, contemplando os softwares Autodesk AutoCAD LT e Autodesk Architecture, Engineering & Construction Collection (AEC Collection).

A indicação dessas soluções justifica-se pelo fato de que o AutoCAD é amplamente utilizado no mercado de engenharia e construção civil, sendo a ferramenta mais difundida para elaboração de projetos técnicos e arquitetônicos, além de possuir compatibilidade com o formato nativo .DWG, amplamente adotado na área.

Além disso, a utilização dessas ferramentas permite:

- padronização dos projetos técnicos conforme normas da ABNT;
- maior eficiência e produtividade na elaboração e revisão de projetos;
- integração com outros profissionais e ferramentas utilizadas no setor de engenharia;
- aproveitamento do conhecimento já existente da equipe técnica da instituição.

Dessa forma, a adoção das soluções Autodesk AutoCAD LT e Autodesk AEC Collection atende de forma mais adequada às necessidades do setor de engenharia do IFSertãoPE.

Da exigência de carta de solidariedade

4.28. Caso o licitante não seja o fabricante da solução ofertada, poderá ser exigida, do licitante provisoriamente classificado em primeiro lugar, carta de solidariedade emitida pelo fabricante ou distribuidor autorizado, declarando responsabilidade solidária quanto ao fornecimento das licenças, atualizações e suporte técnico da solução ofertada, durante todo o período de vigência contratual.

4.29. A exigência aplica-se especialmente às soluções de segurança de rede do fabricante Fortinet, considerando tratar-se de solução proprietária cuja atualização, suporte técnico e acesso às bases de inteligência de segurança dependem de vínculo direto com o fabricante ou seus canais autorizados.

Subcontratação

4.30. Não será admitida a subcontratação do objeto contratual.

Da exigência de amostra

4.31. ~~Havendo o aceite da proposta quanto ao valor, o interessado classificado provisoriamente em primeiro lugar deverá apresentar amostra, que terá data, local e horário de sua realização divulgados por mensagem no sistema, cuja presença será facultada a todos os interessados, incluindo os demais fornecedores interessados.~~

4.32. ~~As amostras poderão ser entregues no endereço [indicar o endereço], no prazo limite de [indicar o prazo], sendo que a empresa assume total responsabilidade pelo envio e por eventual atraso na entrega.~~

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

4.34. ~~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.~~

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

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

4.37. ~~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.~~

4.38. ~~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.~~

4.39. ~~Após a divulgação do resultado final do certame, as amostras entregues deverão ser recolhidas pelos fornecedores no prazo de **XX (xxxxx)** dias, após o qual poderão ser descartadas pela Administração, sem direito a ressarcimento.~~

4.40. ~~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.~~

Garantia da contratação

4.41. 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.

Instalação de escritório

4.42. Não se aplica à presente contratação, considerando que o objeto consiste no fornecimento de licenças de software e serviços associados, cuja execução não demanda a instalação de escritório ou estrutura administrativa local pelo fornecedor.

Margem de Preferência

4.43. Não se aplica à presente contratação, considerando que o objeto se refere ao fornecimento de licenças de software e não se enquadra nas hipóteses de margem de preferência previstas na legislação vigente.

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

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

4.44.1 A solução de segurança de rede deverá contemplar o fornecimento de licenças de Next Generation Firewall (NGFW), incluindo atualização de assinaturas de segurança, suporte técnico e acesso às funcionalidades avançadas da plataforma, pelo período de 60 (sessenta) meses.

4.44.2 A solução deverá ser compatível com a infraestrutura de segurança já existente na instituição, baseada na plataforma Fortinet FortiGate, atualmente utilizada como solução padrão de segurança perimetral nos campi e na Reitoria do IFSertãoPE.

4.44.3 A contratação contempla também o fornecimento de licenças de software CAD, incluindo Autodesk AutoCAD LT e Autodesk Architecture, Engineering & Construction Collection (AEC Collection), pelo período de 36 (trinta e seis) meses, destinadas ao atendimento das demandas do setor de engenharia e elaboração de projetos técnicos da instituição.

4.44.4 As licenças deverão ser fornecidas em formato digital, com ativação por meio do portal do fabricante e acesso às atualizações, correções e suporte técnico durante todo o período contratado.

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

6.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1 Início da execução do objeto: até **5 (cinco) dias úteis após a emissão da Ordem de Serviço.**

6.1.2 A execução compreenderá as seguintes etapas:

- fornecimento das licenças das soluções contratadas;
- ativação das licenças junto aos portais dos fabricantes;

- disponibilização de acesso às plataformas de gerenciamento;
- instalação e configuração inicial da solução de segurança de rede (NGFW);
- integração da solução com a infraestrutura de rede existente;
- validação técnica da solução pela equipe de TI da Contratante;
- disponibilização de suporte técnico e atualizações durante o período contratual.

Local e horário da prestação dos serviços

6.2. Cronograma de realização dos serviços:

Etapa	Prazo
Emissão da Ordem de Serviço	Dia 1
Disponibilização das licenças	até 15 dias
Ativação das licenças	até 5 dias após disponibilização
Implantação e configuração da solução NGFW	até 30 dias
Realização da transferência de conhecimento	até 30 dias após implantação

6.3. Os serviços serão prestados remotamente, por meio de acesso às plataformas e portais dos fabricantes das soluções contratadas.

6.4. Quando necessário, as atividades de implantação da solução NGFW poderão ser realizadas no ambiente de infraestrutura de TI da Contratante.

Rotinas a serem cumpridas

A execução contratual observará as seguintes rotinas:

- monitoramento do funcionamento das licenças e serviços contratados;
- atualização das bases de segurança e assinaturas de ameaças;
- aplicação de atualizações de software disponibilizadas pelos fabricantes;
- atendimento de chamados técnicos abertos pela Contratante;
- manutenção da disponibilidade das funcionalidades contratadas.

Materiais a serem disponibilizados

6.5. Para a perfeita execução do contrato, a contratada deverá disponibilizar:

- licenças digitais das soluções NGFW e Autodesk contratadas;
- acesso aos portais de gerenciamento e administração das soluções;
- documentação técnica, manuais de utilização e guias de configuração das soluções fornecidas.

Informações relevantes para o dimensionamento da proposta

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

6.6.1 fornecimento de licenças da solução de segurança de rede **Next Generation Firewall (NGFW)**, incluindo atualizações de segurança e suporte técnico pelo período de **60 meses**;

6.6.2 fornecimento de licenças de software de engenharia **Autodesk AutoCAD LT e Autodesk AEC Collection**, pelo período de **36 meses**;

6.6.3 disponibilização das licenças em formato digital, com ativação por meio dos portais dos fabricantes e acesso às atualizações e suporte técnico durante todo o período contratual.

Formas de transferência de conhecimento

6.7. A transferência de conhecimento deverá ocorrer durante a fase de implantação da solução NGFW, contemplando:

6.7.1 apresentação da arquitetura da solução e das funcionalidades disponíveis;

6.7.2 capacitação básica da equipe técnica da Contratante para administração da solução;

6.7.3 orientação sobre procedimentos operacionais e boas práticas de segurança.

Procedimentos de transição e finalização do contrato

6.8. Não serão necessários procedimentos específicos de transição ou finalização do contrato, considerando que o objeto consiste no fornecimento de licenças de software e serviços associados, cuja execução não envolve transferência de infraestrutura ou ativos físicos.

Quantidade mínima de serviços para comparação e controle

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

Mecanismos formais de comunicação

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

- I) Ordem de Serviço;
- II) Ata de Reunião;
- III) Ofício;
- IV) Sistema de abertura de chamados;
- V) E-mails;
- VI) Notificações formais.

Manutenção de Sigilo e Normas de Segurança

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

6.12. 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 I e II](#).

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**, considerando que os serviços serão executados predominantemente de forma remota, devendo o preposto permanecer disponível para atendimento às demandas da Contratante durante toda a vigência contratual.

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 **7 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 inexatidão 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 aprazadas, 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 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

7.19. 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.

7.20. 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.

Gestor do Contrato

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

7.21.1 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.

7.21.2 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.

7.21.3 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.

7.21.4 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.

7.21.5 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.

7.21.6 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.

7.21.7 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.

7.21.8 receber e dar encaminhamento imediato:

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

7.21.8.2. 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 **Instrumento de Medição de Resultado (IMR)** para aferição da qualidade da prestação dos serviços relacionados ao suporte técnico e atendimento das demandas registradas pela Contratante.

IAP – ÍNDICE DE ATENDIMENTO NO PRAZO	
Tópico	Descrição
Finalidade	Medir o cumprimento dos prazos de atendimento das solicitações e incidentes registrados pela Contratante junto à Contratada.
Meta a cumprir	IAP igual ou superior a 90%
Instrumento de medição	Sistema de abertura de chamados ou outro mecanismo de registro de atendimento utilizado pela Contratada.
Forma de acompanhamento	Avaliação realizada pelos fiscais do contrato mediante análise dos registros de atendimento.
Periodicidade	Mensal, durante toda a vigência do contrato

Mecanismo de Cálculo (métrica)	$IAP = 100 * (\Sigma Q_{tap} / \Sigma Q_{tr})$ Onde: IAP = Índice de atendimento no prazo ΣQ_{tap} = quantidade de chamados atendidos dentro do prazo ΣQ_{tr} = quantidade total de chamados registrados no período
Início de Vigência	A partir da emissão da OS.
Faixas de ajuste no pagamento e Sanções	$IAP \geq 90\%$ Execução satisfatória $IAP \geq 80\%$ e $< 90\%$ Advertência formal $IAP \geq 70\%$ e $< 80\%$ Multa de até 1% do valor do contrato $IAP < 70\%$ Multa de até 2% do valor do contrato, sem prejuízo de outras sanções

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 da execução contratual para fins de pagamento considerará os seguintes critérios:

8.4.1 disponibilização e ativação das licenças das soluções contratadas;

8.4.2 implantação e funcionamento adequado da solução de segurança de rede (NGFW);

8.4.3 atendimento das solicitações e incidentes registrados pela Contratante dentro dos prazos estabelecidos neste Termo de Referência.

Recebimento

8.5. Os serviços serão recebidos provisoriamente, no prazo de **10 (dez) dias úteis**, 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 os eventos ou etapas de execução do objeto, conforme descrito abaixo:**

I – disponibilização e ativação das licenças das soluções contratadas;

II – implantação e configuração inicial da solução de segurança de rede (NGFW);

III – validação técnica da solução pela equipe da Contratante;

IV – disponibilização do suporte técnico e atualizações das soluções durante o período contratado.

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 **30 (trinta) dias úteis**, 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.

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 das soluções contratadas nos portais dos fabricantes, incluindo acesso às funcionalidades previstas no contrato;

8.22.2 validação do funcionamento da solução de segurança de rede (NGFW), incluindo verificação das funcionalidades de gerenciamento, atualização das bases de segurança e comunicação com a infraestrutura de rede da Contratante;

8.22.3 verificação da disponibilidade das atualizações, suporte técnico e documentação das soluções fornecidas, bem como da conformidade com os requisitos técnicos estabelecidos neste Termo de Referência.

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](#) 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.

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. ~~A presente contratação permite a antecipação de pagamento [parcial] OU [total], conforme as regras previstas no presente tópico.~~

8.40. ~~O Contratado emitirá [recibo] OU [nota fiscal] OU [fatura] OU [documento idôneo] correspondente ao valor da antecipação de pagamento de R\$ **X.XXX,XX** (valor em extenso), tão logo [incluir condicionante – ex: seja assinado o termo de contrato, ou seja, prestada a garantia etc.], para que o Contratante efetue o pagamento antecipado.~~

8.41. ~~Para as etapas seguintes do contrato, a antecipação de pagamento ocorrerá da seguinte forma:~~

8.41.1 ~~R\$ **X.XXX,XX** (valor em extenso)
quando do início da segunda etapa;~~

8.41.2 ~~(...).~~

8.42. ~~Fica o Contratado obrigado a devolver, com correção monetária, a integralidade do valor antecipado na hipótese de inexecução do objeto.~~

8.42.1 ~~No caso de inexecução parcial, deverá haver a devolução do valor relativo à parcela não executada do contrato.~~

8.42.2 ~~O valor relativo à parcela antecipada e não executada do contrato será atualizado monetariamente pela variação acumulada do [especificar o índice de correção monetária a ser adotado], ou outro índice que venha a substituí-lo, desde a data do pagamento da antecipação até a data da devolução.~~

8.43. ~~A liquidação ocorrerá de acordo com as regras do tópico respectivo deste instrumento.~~

8.44. ~~O pagamento antecipado será efetuado no prazo máximo de até **XX (xxxxx)** dias, contados do recebimento do [recibo] OU [nota fiscal] OU [fatura] OU [documento idôneo].~~

8.45. ~~A antecipação de pagamento dispensa o ateste ou recebimento prévios do objeto, os quais deverão ocorrer após a regular execução da parcela contratual a que se refere o valor antecipado.~~

8.46. ~~O pagamento de que trata este item está condicionado à tomada das seguintes providências pelo Contratado:~~

8.46.1 ~~comprovação da execução da etapa imediatamente anterior do objeto pelo Contratado, para a antecipação do valor remanescente;~~

8.46.2 ~~prestação da garantia adicional nas modalidades de que trata o art. 96 da Lei nº 14.133, de 2021, no percentual de **XX% (xxxxx por cento)**.~~

8.47. ~~O pagamento do valor a ser antecipado ocorrerá respeitando eventuais retenções tributárias incidentes.~~

8.48. Não será admitida antecipação de pagamento para a presente contratação, considerando que o pagamento será realizado após a efetiva disponibilização e validação das licenças das soluções contratadas, conforme as condições estabelecidas neste Termo de Referência.

Reajuste

8.49. Os preços registrados na Ata de Registro de Preços serão fixos e irrevogáveis durante sua vigência.

8.50. 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.

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

8.52. 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).

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

8.54. 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.

8.55. 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.

8.56. O reajuste será realizado por apostilamento.

Cessão de Crédito

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

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

8.57.2 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.

8.57.3 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.

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

8.58. 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.

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 esclarecimentos solicitados pela Contratante acerca da execução do objeto.	Multa de 0,2% do valor total do contrato por dia útil de atraso , limitada a 5 dias úteis . Após esse prazo aplica-se multa de 1% do valor total do contrato .
2	Atraso na disponibilização ou ativação das licenças das soluções contratadas.	Multa de 0,5% do valor do item afetado por dia de atraso , limitada a 10% do valor do item .
3	Atraso na implantação ou configuração da solução NGFW.	Multa de 0,5% do valor do item correspondente por dia de atraso , limitada a 10% do valor do item .
4	Não cumprimento dos prazos de atendimento estabelecidos no SLA do suporte técnico.	Multa de 1% do valor do contrato por ocorrência , limitada a 10% do valor total do contrato .

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% (zero vírgula cinco por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 10 (dez) 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 nº 14.133/2021.

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

9.4.4.4. Compensatória, para a inexecução total do contrato prevista 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 na alínea “b”, de 5% (cinco por cento) a 10% (dez por cento) do valor da contratação.

9.4.4.6. Compensatória, em substituição à multa moratória para a infração descrita 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 na alínea “a”, de 1% (um por cento) a 5% (cinco por cento) do valor da contratação.

9.4.4.7.1. Consideram-se infrações enquadráveis nessa alínea, dentre outras:

- atraso na disponibilização das licenças contratadas;
- atraso na implantação ou configuração da solução de segurança de rede;
- descumprimento de prazos de atendimento definidos no Termo de Referência.

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 15 (quinze) 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**.

10.2. O julgamento das propostas será realizado pelo **menor preço por grupo**, considerando a necessidade de contratação conjunta das soluções descritas neste Termo de Referência.

Regime de Execução

10.3. O regime de execução do contrato será por **empreitada por preço global**, considerando que o objeto possui escopo definido e preço previamente estabelecido para fornecimento das licenças e execução dos serviços associados.

Exigências de habilitação

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

Habilitação jurídica

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

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

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

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

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

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

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

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

10.13. 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. Ato de autorização para o exercício da atividade não se aplica à presente contratação, considerando que o objeto consiste no fornecimento de licenças de software e serviços associados, atividade que não está sujeita à autorização específica de órgão regulador.

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

Habilitação fiscal, social e trabalhista

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

10.17. 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.

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

10.19. 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;

10.20. 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;

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

10.22. 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.

10.23. 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

10.24. 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;

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

10.26. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis **do último exercício social**, já exigíveis e apresentados na forma da lei, comprovando, índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas:

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

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

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

10.27. 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, **patrimônio líquido mínimo de 10% (dez por cento) do valor total estimado da contratação.**

10.28. O atendimento aos índices econômicos previstos neste Termo de Referência deverá ser demonstrado com base **no último exercício social apresentado**, 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, devidamente registrado na Junta Comercial ou órgão competente.

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.

10.34. Não se aplica à presente contratação, considerando que o objeto consiste no fornecimento de licenças de software e serviços associados, atividade que não exige registro em conselho ou entidade profissional específica.

10.35. Comprovação de aptidão para o fornecimento de bens e serviços compatíveis com o objeto da contratação, mediante apresentação de atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) que a empresa já executou fornecimento de soluções de tecnologia da informação compatíveis com o objeto desta contratação.

10.35.1. Os atestados apresentados deverão comprovar experiência no fornecimento de licenças de software ou soluções de segurança de rede, compatíveis com o objeto desta contratação.

10.35.2. Para as soluções que dependam de suporte ou licenciamento junto ao fabricante, poderá ser exigida comprovação de vínculo ou autorização do fabricante, quando aplicável.

Qualificação Técnico

10.36. 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.

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

10.36.1.1. fornecimento de licenças de software ou soluções de segurança de rede, compatíveis com o objeto desta contratação;

10.36.1.2. execução de fornecimento de soluções de tecnologia da informação com características semelhantes às previstas neste Termo de Referência.

10.36.2 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.

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

10.36.4 O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do Contratante e local em que foram prestados os serviços, entre outros documentos.

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

10.37. Não se aplica à presente contratação, considerando que os serviços relacionados ao objeto contratado serão executados predominantemente de forma remota, não havendo necessidade de instalação de escritório local pelo fornecedor.

10.38. 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.

10.39. 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.

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

Disposições gerais sobre habilitação

10.41. 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.

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

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

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

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

Documentação complementar para cooperativas

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

10.46.1 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;

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

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

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

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

10.46.6 Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:

10.46.6.1. ata de fundação;

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

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

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

10.46.6.5. três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais;

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

10.46.6.7. 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.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação, que é o máximo aceitável, é de **R\$ 2.177.776,35 (dois milhões, cento e setenta e sete mil, setecentos e setenta e seis reais e trinta e cinco centavos)**, conforme custos unitários apostos na tabela contida no item 1.1 deste Termo de Referência.

11.2. A estimativa de custo levou em consideração os valores obtidos por meio de pesquisa de preços realizada em conformidade com a legislação vigente, bem como o risco envolvido na contratação e sua alocação entre Contratante e Contratado, conforme especificado na matriz de risco constante do contrato.

11.3. O valor possui caráter estimativo, não implicando obrigação de contratação integral.

11.4. 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:

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

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

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

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

12. ADEQUAÇÃO ORÇAMENTÁRIA

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

12.2. A contratação será atendida pela seguinte dotação:

- I) Gestão/unidade: [20RL];
- II) Fonte de recursos: [231742];
- III) Programa de trabalho: [100000000];
- IV) Elemento de despesa: [339040]; e
- V) Plano interno: [L20RLP01FUN].

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

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

13. DISPOSIÇÕES FINAIS

13.1. As informações contidas neste Termo de Referência **não são classificadas como sigilosas**, nos termos da legislação vigente.

Cronograma Físico Financeiro

Evento	Prazo estimado	Valor
Evento 1 – Emissão da Ordem de Serviço	Até 5 dias após assinatura do contrato ou instrumento equivalente	Sem impacto financeiro
Evento 2 – Disponibilização e ativação das licenças das soluções contratadas (NGFW e Autodesk)	Até 15 dias após emissão da Ordem de Serviço	Conforme valor do item contratado
Evento 3 – Implantação e configuração inicial da solução de segurança de rede (NGFW)	Até 30 dias após disponibilização das licenças	Conforme valor do serviço contratado
Evento 4 – Aceite técnico da solução pela Contratante	Após validação técnica da equipe de TI	Liberação para faturamento

Evento 5 – Disponibilização de suporte técnico e atualizações das soluções	Durante todo o período contratual (36 ou 60 meses)	Incluído no valor das licenças
--	--	--------------------------------

Integrante Requisitante Klemmerson Amariz Gomes SIAPE: 1191344	Integrante Técnico Melquizedequi Cabral dos Santos SIAPE: 1620645	Integrante Administrativo Herica Vanessa Fonseca Silva SIAPE:2156605
--	---	--

Autoridade Máxima da Área de TIC
Francisco Hamilton de Freitas Junior Diretor de TI SIAPE: 1780810

Petrolina, 10 de março de 2026

Aprovo,

Autoridade Competente

Jean Carlos Coelho de Alencar
Reitor
SIAPE: 2671023