

Termo de Referência 50/2025

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
50/2025	158149-INST.FED.EDUC.CIENC.E TEC.SERTão PERNAMBUCANO	FRANCISCO HAMILTON DE FREITAS JUNIOR	20/05/2026 10:17 (v 0.11)
Status	ASSINADO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC	27/2025	23302.101823/2025-19

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

Referência: Arts. 12 a 24 da Instrução Normativa SGD/ME nº 94, de 2022

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União - CNMLC  
Atualização: maio/2023  
Termo de Referência contratação de Serviços TIC - Licitação  
Elaborado pela Secretaria de Gestão. Complementado e Uniformizado pela CNMLC  
Identidade visual pela Secretaria de Gestão

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. Conforme especificações e condições constantes deste termo de referência e seus anexos.

VALORES ESTIMADOS   Grupo 01						
Grupo 01	ITEM	ESPECIFICAÇÃO	CATSER	TOTAL (A)	VALOR UNITÁRIO (R\$) 60 meses (B)	VALOR TOTAL (R\$) AXB
	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.	27502	5	R\$	R\$
	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.	27502	1	R\$	R\$
		Serviço de Fornecimento de Licença para Solução Integrada de Proteção de Rede para Segurança de Informação: Next Generation				

	03	Firewall (NGFW) – Tipo 3 com atualização por 60 (sessenta) meses.	27502	2	R\$	R\$
	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.	27502	1	R\$	R\$
	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	R\$	R\$
	06	Serviço de Instalação, configuração e repasse de conhecimento	26972		R\$	R\$
<b>TOTAL GERAL</b>						

1.2. O (s) serviço (s) objeto desta contratação são caracterizados como comuns, uma vez que as soluções a serem adquiridas encontram-se disponíveis no mercado, ou seja, possuem especificações usuais, podendo definir seus padrões de desempenho, características e qualidades de forma objetiva, garantindo assim competitividade para sua prestação.

1.3 O prazo de vigência da contratação é de 60 (sessenta) meses para os itens do Grupo 01 contados da assinatura do contrato, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

1.3.1. 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.

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

## 2. DESCRIÇÃO DA SOLUÇÃO

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

2.2. 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.

2.3. 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.

2.4. 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.

	ITEM	ESPECIFICAÇÃO	CATSER	TOTAL
Grupo 01	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.  Part Number: FC2-10-AZVMS-465-01-60	27502	1
06	Serviço de Instalação, configuração e repasse de conhecimento	26972	6

O agrupamento dos itens em lote único justifica-se pela necessidade de fornecimento de solução integrada de segurança de rede, composta por equipamentos, licenciamento, subscrições, suporte técnico e demais componentes que operam de forma interdependente e integrada.

O parcelamento dos itens poderá ocasionar incompatibilidade entre versões, falhas de interoperabilidade, fragmentação do suporte técnico, dificuldades na gestão contratual e riscos à continuidade dos serviços de segurança da informação do IFSertãoPE.

O parcelamento da contratação não se mostra tecnicamente viável em razão da integração nativa entre os componentes da solução Fortinet Security Fabric, da necessidade de gerenciamento unificado, da compatibilidade operacional entre os itens e da necessidade de suporte técnico centralizado.

A contratação em grupo único assegura padronização tecnológica, suporte centralizado, garantia de funcionamento integrado da solução, simplificação administrativa da fiscalização contratual e maior eficiência operacional, sem prejuízo da competitividade do certame, considerando a existência de fornecedores aptos à entrega integral da solução.

### **Descrição Detalhada**

Item	Descrição
	<p><b>Firewall UTM – Tipo 1 - VM2</b></p> <p>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.</p> <p><b>REQUISITOS GERAIS</b></p> <p>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.</p> <p>Deverá estar licenciado para no mínimo 2 (dois) vCPU cores.</p> <p>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.</p> <p>O Sistema Operacional do firewall deve ser capaz de adicionar novas funcionalidades sem a necessidade de reinstalação da solução.</p> <p>Os componentes da solução (incluindo o sistema operacional, drivers de dispositivos e aplicativos de segurança) devem ser desenvolvidos, produzidos e comercializados pela mesma fabricante.</p> <p>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.</p> <p>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.</p> <p>A solução deve ter integração com diretórios LDAP para autenticação e autorização de usuários baseado nos perfis armazenados no LDAP ou no firewall.</p> <p>Deve incluir a funcionalidade de pesquisar múltiplos servidores de LDAP para redundância e encontrar usuários distribuídos em múltiplos servidores de LDAP.</p> <p>O sistema operacional deve implementar política de senha de usuário administrador, com os seguintes requisitos:</p> <ul style="list-style-type: none"> <li>• Deve ser capaz de impor um tamanho mínimo e os diferentes tipos de caracteres (números, letras, caracteres especiais);</li> <li>• Deve ser capaz de forçar mudanças de senha periódica;</li> <li>• Deve acompanhar o histórico de senhas “velhas” para evitar a reutilização delas;</li> </ul>

- 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 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.

01

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.

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 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.

#### **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 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 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.

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.

O período de disponibilidade para chamada dos serviços de manutenção dos equipamentos é de 24 horas por dia, 7 dias por semana.

### **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 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.

03

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.

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.

O período de disponibilidade para chamada dos serviços de manutenção dos equipamentos é de 24 horas por dia, 7 dias por semana.

#### **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**

- 04** 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.
- 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.

#### **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;

05

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;

#### **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.

#### **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 poderá 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:

06

- 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;
- 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;

### 3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE

**3.1. Justificativa para padronização:** 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.

A padronização tecnológica observada nesta contratação encontra respaldo no art. 41, inciso I, da Lei nº 14.133/2021, considerando a necessidade de compatibilidade técnica, integração operacional, continuidade da solução existente e preservação dos investimentos já realizados pela Administração.

3.2. O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme detalhamento a 3.2 seguir:

**I) ID PCA no PNCP:** 10830301000104-0-000009/2025

**II) Data de publicação no PNCP:** 13/05/2024

**III) Id do item no PCA:** 22

**IV) Classe/Grupo:** 182 - SERVIÇOS DE LICENCIAMENTO E CONTRATOS DE TRANSFERÊNCIA DE TECNOLOGIA

**V) Identificador da Futura Contratação:** 158149-27/2025

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

3.4. 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.)

## 4. REQUISITOS DA CONTRATAÇÃO

### Requisitos de Negócio:

- 4.2. A presente contratação orienta-se pelos seguintes requisitos de negócio:
- 4.2.1. Atender a demanda crescente por prevenção e mitigação de incidentes de segurança da informação;
  - 4.2.2. Garantir a adequação dos serviços de TI com os atos normativos do Governo Federal (LGPD, marco civil da internet, política nacional de segurança da informação, etc.);
  - 4.2.3. Manter a disponibilidade, integridade e confiabilidade dos sistemas e aplicações da instituição;
  - 4.2.4. Garantir o funcionamento da rede institucional em regime de 24x7 ininterruptamente, com troca de equipamentos em até 24 horas após notificação do fabricante;

### Requisitos de Capacitação

- 4.3. Deverão ser realizadas reuniões de ponto de controle, sob demanda, para solução de dúvidas sobre a gestão o ambiente entre a CONTRATADA e o IFSertãoPE.
- 4.4. 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

- 4.5. 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 de Manutenção



4.7. O prazo de garantia será aquele previsto na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), sem prejuízo das demais garantias ofertadas pelo fabricante e pela CONTRATADA. A solução de segurança de rede deverá possuir garantia, suporte técnico e manutenção durante toda a vigência contratual de 60 (sessenta) meses, contemplando obrigatoriamente os seguintes requisitos:

- **RGM01 – Garantia das licenças e serviços** : A CONTRATADA deverá garantir a validade, autenticidade e pleno funcionamento das licenças fornecidas da solução integrada de proteção de rede NGFW, incluindo os módulos de gerenciamento centralizado e análise de logs, durante todo o período contratual.
- **RGM02 – Atualizações de segurança** : A solução deverá possuir acesso contínuo às atualizações de assinaturas, bases de ameaças, mecanismos de detecção, firmwares, patches de segurança e novas versões disponibilizadas pelo fabricante, sem custos adicionais para a CONTRATANTE.
- **RGM03 – Suporte técnico especializado** : A CONTRATADA deverá disponibilizar suporte técnico especializado para atendimento de incidentes, falhas operacionais, dúvidas técnicas e problemas relacionados à instalação, configuração, integração e funcionamento da solução NGFW.
- **RGM04 – Atendimento de chamados** : Os chamados técnicos poderão ser abertos pela CONTRATANTE por meio eletrônico, telefônico ou portal de atendimento disponibilizado pela CONTRATADA, durante toda a vigência contratual.
- **RGM05 – Correção de falhas** : A CONTRATADA deverá atuar na identificação, diagnóstico e correção de falhas, vulnerabilidades ou inconsistências que comprometam a disponibilidade, integridade, confidencialidade ou desempenho da solução contratada.
- **RGM06 – Manutenção preventiva e evolutiva** : A solução deverá permitir manutenção preventiva, corretiva e evolutiva, incluindo atualização tecnológica dos componentes licenciados, conforme disponibilizações oficiais do fabricante, sem interrupção indevida dos serviços institucionais.
- **RGM07 – Continuidade operacional** : A CONTRATADA deverá assegurar a continuidade operacional da solução de segurança de rede, garantindo a manutenção das funcionalidades contratadas e das políticas de proteção implementadas no ambiente da CONTRATANTE.
- **RGM08 – Compatibilidade tecnológica** : As atualizações e correções disponibilizadas não poderão causar incompatibilidade com o ambiente tecnológico atualmente utilizado pela CONTRATANTE, devendo ser mantida a interoperabilidade da solução com a infraestrutura existente.
- **RGM09 – Transferência de conhecimento** : Sempre que houver alterações relevantes na solução decorrentes de atualização tecnológica ou implementação de novas funcionalidades, a CONTRATADA deverá fornecer orientações técnicas e repasse de conhecimento à equipe da CONTRATANTE, quando solicitado.
- **RGM10 – Documentação técnica** : A CONTRATADA deverá disponibilizar documentação técnica atualizada, manuais, guias de configuração e demais informações necessárias para operação e administração da solução fornecida.

4.8. Os serviços de suporte técnico abrangem:

- 4.8.1. O atendimento deve ser 24x7x365, ou seja, 24 (vinte e quatro) horas por dia em 7 (sete) dias da semana por 365 (trezentos e sessenta e cinco) dias por ano, em língua portuguesa;
- 4.8.2. Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;
- 4.8.3. Elaboração de relatórios, estudos e diagnósticos sobre o ambiente;
- 4.8.4. Transferência de conhecimento aos técnicos da CONTRATANTE referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes;
- 4.8.5. Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.
- 4.8.6. O suporte técnico contempla o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução.
- 4.8.7. O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação etc.) necessários ao funcionamento da solução;

4.9. 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;

4.10. 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.

4.11. 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.

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

<b>Atividade, Tarefa ou Serviço</b>	<b>Prazo máximo de início de atendimento</b>	<b>Prazo máximo de solução de problema</b>
<i>Realização de Reunião Inicial</i>	<i>Até 7 (sete) dias úteis da assinatura do contrato.</i>	<i>Até 14 (quatorze) dias úteis da assinatura do contrato.</i>
<i>Emissão da Ordem de Serviço</i>	<i>Na reunião inicial ou até 05 (cinco) dias úteis após esta, a critério da Administração.</i>	<i>10 (dez) dias úteis após esta, a critério da Administração.</i>
<i>Entrega da Solução</i>	<i>10 (dez) dias corridos iniciando da data de emissão da Ordem de Serviço.</i>	<i>10 (dez) dias corridos iniciando da data de emissão da Ordem de Serviço.</i>
<i>Aceite Provisório</i>	<i>Até 15 (quinze) dias corridos após a configuração, instalação e disponibilidade para utilização.</i>	<i>Até 15 (quinze) dias corridos após a configuração, instalação e disponibilidade para utilização.</i>
<i>Aceite Definitivo</i>	<i>Até 15 (quinze) dias corridos após a emissão do Termo de Recebimento Provisório e verificação da qualidade da solução entregue.</i>	<i>Até 15 (quinze) dias corridos após a emissão do Termo de Recebimento Provisório e verificação da qualidade da solução entregue.</i>

### **Requisitos de Segurança e Privacidade**

4.13. 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:

4.13.1. 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;

4.13.2. 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.

4.14. 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-dedados/guias/guia\\_requisitos\\_obrigacoes.pdf/view](https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-dedados/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**

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

4.15.1. 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.

4.15.2. 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.

4.15.3. 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.

4.15.4. A presente contratação deverá prezar, sempre que possível, por documentos em meios digitais em detrimento ao uso de papel impresso.

4.16. O acesso aos serviços deverá estar disponível no idioma Português do Brasil.

### **Requisitos da Arquitetura Tecnológica**

4.17. Os serviços deverão ser executados observando-se a arquitetura tecnológica atualmente adotada pelo IFSertãoPE, baseada na plataforma Fortinet/FortiGate já implantada nas unidades da instituição, garantindo compatibilidade, interoperabilidade, gerenciamento

centralizado e integração com os componentes existentes da infraestrutura de segurança da informação.

4.18. Não será admitida solução incompatível com a arquitetura tecnológica e com a plataforma de segurança Fortinet/FortiGate atualmente utilizada pelo IFSertãoPE, salvo mediante comprovação técnica inequívoca de compatibilidade plena e autorização formal da CONTRATANTE.

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

#### **Requisitos de Projeto e de Implementação**

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

4.20.1. A CONTRATANTE deverá manter equipe técnica responsável pelo acompanhamento da execução contratual, cabendo à CONTRATADA realizar o fornecimento, ativação, configuração, atualização, integração e operacionalização das licenças e serviços da solução de segurança já existente no ambiente institucional, bem como efetuar os repasses de conhecimento necessários à equipe técnica da CONTRATANTE.

4.20.2. A CONTRATADA deverá disponibilizar profissional técnico responsável pelo acompanhamento da ativação e integração da solução licenciada no IFSertãoPE, a fim de tratar das questões técnicas e administrativas.

4.20.3. O recebimento dos itens licitados se dará:

4.20.3.1. 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:

4.20.3.1.1. Ativação das licenças;

4.20.3.1.2. Comprovação de que as licenças fornecidas atendem às especificações mínimas exigidas ou aquelas superiores oferecidas;

4.20.3.1.3. Comprovação de que os certificados de garantia atendem às especificações mínimas exigidas;

4.20.3.1.4. Transferência de conhecimento aos técnicos da CONTRATANTE;

4.20.3.2. 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.

4.20.4. 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**

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

4.21.1. Para a implantação dos itens a serem contratados, deverá ser provido pela empresa CONTRATADA a transferência de conhecimentos dos procedimentos operacionais que serão realizados.

4.21.2. A transferência deverá contemplar os seguintes itens:

4.21.2.1. Apresentação da solução a ser implementada;

4.21.2.2. Plano de instalação da solução, que contemple todas as atividades a serem realizadas para garantir o menor impacto possível aos ambientes de produção do IFSertãoPE;

4.21.2.3. Operação e Administração da solução;

4.21.2.4. Descrição e uso das funcionalidades da solução;

4.21.2.5. Resolução de problemas;

4.21.2.6. Procedimentos de manutenção (atualizações de software);

4.21.3. A CONTRATADA e o IFSertãoPE elaborarão em conjunto um cronograma contendo as datas e horários para realização do repasse de conhecimento da solução, que deverá também atender às seguintes exigências:

4.21.3.1. A solução e todos os seus elementos deverão ser instalados, configurados, migrados, integrados e otimizados, segundo as melhores práticas do fabricante em termos de desempenho, disponibilidade e segurança, por técnico qualificado por este, de modo a garantir total interoperabilidade no ambiente computacional do IFSertãoPE;

4.21.3.2. Concluídos os serviços de instalação e configuração, deverão ser realizados testes de operação com todas as tecnologias envolvidas na solução, durante período de até 5 (cinco) dias corridos seguintes à instalação, de modo a garantir total interoperabilidade no ambiente computacional do IFSertãoPE objetivando a comprovação dos itens fornecidos e suas respectivas funcionalidades. Os resultados dos testes deverão ser incluídos na documentação a ser entregue;

4.21.3.3. A CONTRATADA será a responsável pela implantação ou reimplementações do produto nas dependências do IFSertãoPE;

4.21.3.4. O objeto deste item deve ser implantado ou reimplantado nas dependências do IFSertãoPE;

4.21.3.5. Deve haver a otimização dos recursos para que haja a adequação do produto à infraestrutura disponibilizada;

4.21.3.6. Implantações ou reimplementações deverão ser realizadas durante todo o período de validade da licença;

- 4.21.3.7. Apoio para desinstalação de soluções de proteção de outros fabricantes;
- 4.21.3.8. A liberação da licença e a entrega do software poderão ser realizadas através de download pela internet, preferencialmente pelo site do fabricante do software, com prévio agendamento por meio do e-mail [redes@ifsertao-pe.edu.br](mailto:redes@ifsertao-pe.edu.br);

### **Requisitos de Garantia e Manutenção**

4.22. 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.

- 4.22.1. Os serviços de garantia e de manutenção e suporte deverão ser capazes de assegurar o funcionamento da solução de segurança CONTRATADA, com todas as suas funcionalidades, durante toda a vigência do contrato, com suporte e manutenção corretiva sob demanda.
- 4.22.2. O fabricante/fornecedor deverá manter suporte técnico (para resolução de dúvidas e problemas) em português, durante todo o prazo de vigência do contrato.

### **Requisitos de Experiência Profissional**

4.23. 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**

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

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

### **Requisitos de Metodologia de Trabalho**

- 4.25. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela CONTRATANTE.
- 4.26. A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.
- 4.27. 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.
- 4.28. A execução do serviço deve ser acompanhada pelo CONTRATADO, que dará ciência de eventuais acontecimentos à CONTRATANTE.

- 4.28.1. A metodologia de trabalho deverá seguir o disposto nos requisitos de negócio e tecnológicos.

### **Requisitos de Segurança da Informação e Privacidade**

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

- 4.29.1. A CONTRATADA deverá respeitar as diretrizes constantes da Política de Segurança da Informação (POSIN) do IFSertãoPE em vigência;
- 4.29.2. 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;
- 4.29.3. 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;

4.30. 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**

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

### **Sustentabilidade**

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

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

#### **Subcontratação**

4.33. Não é admitida a subcontratação do objeto contratual.

#### **Garantia da Contratação**

4.34. Não haverá exigência de garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133/2021, considerando que o objeto consiste predominantemente no fornecimento de licenças de software e serviços associados de suporte e atualização tecnológica, possuindo baixo risco de inadimplemento contratual.

4.35. Ademais, a contratação prevê mecanismos de controle, aceite técnico, fiscalização contratual e aplicação de sanções administrativas, considerados suficientes para resguardar os interesses da Administração.

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

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

4.36.1. O IFSertãoPE possui a necessidade da contratação de empresa especializada no fornecimento de licenças de software de solução de proteção de estações de trabalho/servidores incluindo implantação da solução, treinamento, manutenção especializada e suporte técnico.

## **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 Fornecedor 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, contendo:

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

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

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

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

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

5.3.4.3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 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.

5.3.5. Não será admitida adesão à Ata de Registro de Preços por órgãos ou entidades não participantes, considerando a natureza especializada da solução de TIC contratada, os quantitativos planejados para atendimento da demanda institucional e as disposições da Instrução Normativa SGD/ME nº 94/2022.

## **6. MODELO DE EXECUÇÃO DO CONTRATO**

### **Condições de execução**

6.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1. O início da execução do objeto ocorrerá em até 5 (cinco) dias úteis após a emissão da Ordem de Serviço, prazo no qual a CONTRATADA deverá iniciar os procedimentos administrativos, operacionais e técnicos necessários à disponibilização da solução.

6.1.2. A disponibilização integral das licenças e funcionalidades contratadas deverá ocorrer em até 15 (quinze) dias úteis após a emissão da Ordem de Serviço.

6.1.3. Cronograma de realização dos serviços:

6.1.4. A Entrega da Solução terá de ser realizada em no máximo 10 (dez) dias corridos após a formalização do pedido.

6.1.5. O Termo de Recebimento Provisório será emitido no prazo de 15 (quinze) dias corridos a contar da entrega do relatório mensal pela CONTRATADA, e consistirá na declaração formal de que os serviços foram prestados, para posterior análise das conformidades e qualidades baseadas nos requisitos e nos critérios de aceitação.

6.1.6. O Termo de Recebimento Definitivo será emitido no prazo de 15 (quinze) dias corridos após o recebimento provisório e consistirá na declaração formal de que os serviços prestados atendem aos requisitos estabelecidos e aos critérios de aceitação.

6.1.7. A execução do contrato não gerará vínculo empregatício em nenhuma hipótese com a CONTRATADA.

### **Local e horário da prestação dos serviços**

6.2. Os serviços serão prestados no seguinte endereço:

6.2.1. O objeto do contrato será executado de maneira remota, em instalações de responsabilidade da CONTRATADA.

6.3. Os serviços serão prestados no seguinte horário:

6.3.1. Para fins de horário de atendimento técnico, considera-se o período de 24x7 (24 horas por dia, 7 dias na semana).

#### **Materiais a serem disponibilizados**

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

6.4.1. À CONTRATADA caberá fornecer todos os demais recursos e condições técnicas necessárias à execução dos serviços.

#### **Informações relevantes para o dimensionamento da proposta**

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

6.5.1. As informações encontra-se no item 2.4;

#### **Formas de transferência de conhecimento**

6.6. A transferência do conhecimento deverá ser realizada observando-se os Requisitos de Capacitação.

#### **Procedimentos de transição e finalização do contrato**

6.7. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:

6.7.1. Durante os 30 (trinta) dias anteriores ao encerramento do contrato, a CONTRATADA se comprometerá a participar do processo de transição dos serviços contratados, em conjunto com a empresa sucessora e a CONTRATANTE, disponibilizando todas as informações pertinentes ao serviço de forma a permitir sua continuidade sem prejuízo ao funcionamento dos sistemas do órgão.

6.8 A CONTRATADA deverá apresentar todas as informações que lhe forem solicitadas pelas CONTRATANTE para os procedimentos de transição e finalização do contrato.

#### **Quantidade mínima de serviços para comparação e controle**

6.9 Os quantitativos para dos itens que compõem a solução são aqueles expressos no item 2.4 deste TR.

#### **Mecanismos formais de comunicação**

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

- 6.10.1. Ordem de Serviço;
- 6.11.2. Ata de Reunião;
- 6.12.3. Ofício;
- 6.13.4. Sistema de abertura de chamados;
- 6.14.5. E-mails e Cartas

#### **Formas de Pagamento**

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

#### **Manutenção de Sigilo e Normas de Segurança**

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

6.13. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos **ANEXOS 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 representante da empresa para adoção de providências que devam ser cumpridas de imediato.

### Preposto

7.5. A CONTRATADA 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 preposto da empresa será o responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder às principais questões técnicas, legais e administrativas referentes ao andamento contratual.

7.7. CONTRATANTE poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a CONTRATADA 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 (sete) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da CONTRATANTE.

7.9.1. A pauta desta reunião observará, pelo menos:

7.9.1.1. Presença do representante legal da CONTRATADA, que apresentará o seu preposto;

7.9.1.2. Entrega, por parte da CONTRATADA, do Termo de Compromisso e dos Termos de Ciência;

7.9.1.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.9.1.4. 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;

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

### Fiscalização

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

### Fiscalização Técnica

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

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

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

7.11.3 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. (**Decreto nº 11.246, de 2022, art. 22, IV**)

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



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

### **Fiscalização Administrativa**

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

7.12.1 Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; **(Decreto nº 11.246, de 2022, art. 23, IV )**.

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

7.13.1 Receber, conferir e acompanhar o material/serviços recebidos/prestados; e

7.13.2 Atestar os materiais/serviços recebidos/prestados.

### **Gestor do Contrato**

7.14 O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. **(Decreto nº 11.246, de 2022, art. 21, IV)**

7.15 O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. **(Decreto nº 11.246, de 2022, art. 21, II)**

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

7.17 O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. **(Decreto nº 11.246, de 2022, art. 21, VIII)**

7.18 O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. **(Decreto nº 11.246, de 2022, art. 21, X)**

7.19 O gestor do contrato deverá 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. . **(Decreto nº 11.246, de 2022, art. 21, VI)**

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

## **8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO**

8.1. A avaliação da execução do objeto será realizada pela fiscalização contratual mediante verificação da disponibilização integral da solução contratada, ativação das licenças, funcionamento das funcionalidades previstas, suporte técnico e atendimento aos requisitos técnicos estabelecidos neste Termo de Referência.

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

- 8.2.1. não produzir os resultados acordados;
- 8.2.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou
- 8.2.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los 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. Disponibilidade do serviço.

8.4.2. Execução do contrato

8.4.3. O pagamento das licenças, máquinas virtuais, subscrições e serviços agregados da solução de segurança de rede será realizado em parcela única, após a disponibilização integral da solução contratada, ativação das licenças e funcionalidades, validação técnica pela fiscalização do contrato e emissão do Termo de Recebimento Definitivo.

8.4.4. A CONTRATADA deverá assegurar a manutenção do suporte técnico, atualizações de segurança, assinaturas, funcionalidades e disponibilidade da solução durante toda a vigência contratual.

8.4.5. Em caso de perda de acesso às licenças, indisponibilidade da solução, descontinuidade do suporte técnico, ausência de atualização tecnológica ou encerramento antecipado da prestação contratual por responsabilidade da CONTRATADA, poderão ser aplicadas as sanções administrativas cabíveis, inclusive devolução proporcional dos valores pagos relativos ao período não executado, sem prejuízo das demais penalidades previstas neste Termo de Referência e na legislação aplicável.

#### **Do recebimento**

8.5 Os serviços serão recebidos provisoriamente, no prazo de 30 dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. **(Art. 140, I, a, da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022)**

8.5.1 O prazo da disposição acima 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.

8.6 O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. **(Art. 22, X, Decreto nº 11.246, de 2022)**

8.7 O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. **(Art. 23, X, Decreto nº 11.246, de 2022)**

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

8.9 Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá 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, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

8.9.1 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;

8.10 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.

8.11 A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. **(Art. 119 c/c art. 140 da Lei nº 14133, de 2021)**

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

8.13 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.

8.14 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.

8.15 Os serviços serão recebidos definitivamente no prazo de 30 dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

8.15.1 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 **(art. 21, VIII, Decreto nº 11.246, de 2022)**

8.15.2 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 à Contratada, por escrito, as respectivas correções;

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

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

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

8.16 No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do , comunicando-se à empresa para emissão **art. 143 da Lei nº 14.133, de 2021** de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

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

8.18 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.

8.19 Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

8.19.1 inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

8.19.2 ensejar o retardamento da execução do objeto;

8.19.3 fraudar na execução do contrato;

8.19.4 comportar-se de modo inidôneo;

8.19.5 cometer fraude fiscal;

8.19.6 não manter a proposta.

8.20 A Contratada que cometer qualquer das infrações discriminadas nos subitens acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

8.20.1 advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

8.20.2 multa moratória de 0,33% do valor mensal contratado, por atraso injustificado na implantação e liberação do sistema para uso do contratante, até o limite de 10% (dez por cento) do valor contratado.

8.20.3 multa compensatória de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

8.20.4 em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

8.20.5 suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

8.20.6 declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

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

8.22 As penalidades serão obrigatoriamente registradas no SICAF.

## Procedimentos de Teste e Inspeção

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

8.23.1. A solução será aceita provisória e definitivamente, conforme os prazos e condições estabelecidos no item 4.12. Poderá ser solicitado ainda esclarecimentos à CONTRATADA em casos de dúvidas para fins de verificação de conformidade, além de solicitação de testes que demonstrem o pleno funcionamento da solução. Em caso de não conformidade, a CONTRATANTE solicitará à CONTRATADA que refaça quaisquer operações necessárias ao pleno funcionamento da solução, sem prejuízo da aplicação de eventuais glosas e penalidades previstas neste Termo de Referência.

8.23.2. A qualidade do serviço na fase de execução contratual será avaliada pelos fiscais do contrato, os quais reportarão ao gestor possíveis falhas na prestação do serviço.

## Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

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

8.24.2.1. **Advertência**, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

8.24.2.2. **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

8.24.2.3. **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

8.24.2.4. **Multa**:

- Moratória de 10% (dez por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 60 (sessenta) dias;
  - Moratória de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso injustificado, até o máximo de 2% (dois por cento) pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.
1. a) O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

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

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

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

## Liquidação

8.26 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, §2º da Instrução Normativa SEGES/ME nº 77/2022

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

8.28 Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

8.28.1 o prazo de validade;

8.28.2 a data da emissão;

8.28.3 os dados do contrato e do órgão contratante;

8.28.4 o período respectivo de execução do contrato;

8.28.5 o valor a pagar; e

#### 8.28.6 eventual destaque do valor de retenções tributárias cabíveis.

8.29 Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

8.30 A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

8.31 A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas. (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018)

8.32 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.

8.33 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.

8.34 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.

8.35 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**

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

8.37 No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice de correção monetária. IPCA

#### **Forma de pagamento**

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

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

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

8.41 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.

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

#### **Cessão de crédito**

8.43 É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.

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

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

8.46 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 JL01, de 18 de maio de 2020.

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

8.48 Os preços inicialmente contratados são fixos e irrevogáveis no prazo de um ano contado da data do orçamento estimado.

## 9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

### Forma de seleção e critério de julgamento da proposta

9.1. 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, em conformidade com a Lei 14.133/2021, artigo 31º, inciso I.

### Regime de execução

9.2. O regime de execução do contrato será por empreitada por preço unitário.

9.2.1. A adoção do regime de empreitada por preço unitário justifica-se em razão da contratação ocorrer por meio do Sistema de Registro de Preços, com quantitativos estimados e possibilidade de fornecimento parcelado conforme a necessidade da Administração e dos órgãos participantes.

### Da Aplicação da Margem de Preferência

9.3. Aplica-se a margem de preferência conforme descrito a seguir:

9.4. Será assegurado o direito de preferência, no caso de empate, para microempresas e empresas de pequeno porte de que tratam o artigo 44 da Lei Complementar nº 123, de 14 de dezembro de 2006, desde que atendido aos requisitos deste Termo de Referência.

### Exigências de habilitação

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

#### Habilitação jurídica

9.6. **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;

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

9.8. **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>;

9.9. **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;

9.10. **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.

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

9.12. **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

9.13. **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 de 1971.

9.14. **Produtor Rural:** matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB n. 971, de 13 de novembro de 2009 (arts. 17 a 19 e 165).

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

#### Habilitação fiscal, social e trabalhista

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

9.17. 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.

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

9.19. 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;

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

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

9.22. Caso o fornecedor seja considerado isento dos tributos [Estadual/Distrital] ou [Municipal/Distrital] relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

9.23. 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.

#### **Habilitação fiscal, social e trabalhista**

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

9.25. 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.

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

9.27. 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;

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

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

9.30. Caso o fornecedor seja considerado isento dos tributos Estadual/Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

9.31. 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**

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

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

9.34. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

9.34.1. Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

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

9.34.3. 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.

9.34.4. 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.

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

9.36. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

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

Qualificação Técnica

9.38. Comprovação de aptidão para execução de serviço compatível em características, quantidades e complexidade tecnológica com o objeto desta contratação, mediante apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

9.38.1. Para fins da comprovação de que trata este subitem, os atestados deverão demonstrar experiência no fornecimento de solução de segurança de rede do tipo Next Generation Firewall (NGFW) ou solução equivalente, incluindo licenciamento, suporte técnico e atualização de assinaturas de segurança.

9.38.2. Será admitido o somatório de atestados para fins de comprovação da capacidade técnica do fornecedor.

9.38.3. Os atestados poderão ser apresentados em nome da matriz ou da filial do fornecedor.

9.38.4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, podendo a Administração realizar diligências para verificação das informações prestadas.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1 O custo estimado total da contratação 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)** por 60 meses relacionado Licenças da Fortigate da Fortinet , conforme custos unitários apostos na tabela abaixo e documento em anexo.

VALORES ESTIMADOS   Grupo 01						
Grupo 01	ITEM	ESPECIFICAÇÃO	CATSER	TOTAL (A)	VALOR UNITÁRIO (R\$)  60 meses  (B)	VALOR TOTAL (R\$)  AXB
	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.	27502	05	R\$ 111.500,40	R\$ 557.502,00
	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.	27502	02	R\$ 206.528,00	R\$ 413.056,00
	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.	27502	02	R\$ 501.194,30	R\$ 1.002.388,60
	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.	27502	01	R\$ 23.079,75	R\$ 23.079,75
	05	Licença para solução integrada de proteção de Rede para segurança de informação: Software de gerenciamento centralizado com atualização por 60 sessenta meses.	27502	01	R\$ 45.250,00	R\$ 45.250,00
	06	Serviço de Instalação, configuração e repasse de conhecimento	26972	06	R\$ 22.750,00	R\$ 136.500,00
	TOTAL GERAL					R\$ 2.177.776,35

11. ADEQUAÇÃO ORÇAMENTÁRIA

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

11.2 A contratação será atendida pela seguinte dotação:

- PROGRAMA/AÇÃO: 20RL



- **PLANO DE TRABALHO RESUMIDO:** 231742
- **FONTE DE RECURSOS:** 100000000
- **NATUREZA DA DESPESA:** 339040
- **PLANO INTERNO:** L20RLP01FUN

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

**Cronograma Físico Financeiro**

Evento	Prazo estimado	Valor
Evento 1	<del>(.../.../...) a (.../.../...) ou (...) dias após a emissão da OS</del>	R\$ .....
Evento 2	[...]	R\$ .....
Evento N	[...]	R\$ .....

11.4 A Ata de Registro de Preços decorrente desta contratação terá vigência de 12 (doze) meses, podendo ser prorrogada por igual período, desde que comprovada a vantajosidade, nos termos do art. 84 da Lei nº 14.133/2021 e do Decreto nº 11.462/2023.

Os quantitativos registrados representam a estimativa de consumo durante a vigência da ata, considerando as demandas do órgão gerenciador e dos órgãos participantes.

Em caso de prorrogação da ata, poderá haver a renovação dos quantitativos inicialmente registrados, no todo ou em parte, mediante justificativa da Administração e demonstração da vantajosidade dos preços registrados, conforme legislação vigente.

A utilização dos quantitativos registrados ocorrerá de forma parcelada, conforme a necessidade da Administração, não havendo obrigação de contratação integral dos quantitativos estimados.

**12. CLÁUSULA ANTICORRUPÇÃO**

CLÁUSULA DECLARATÓRIA E COMPROMISSÓRIA ANTICORRUPÇÃO A SER INCLUÍDA NOS INSTRUMENTOS PACTUADOS "DA LEI ANTICORRUPÇÃO.

As partes **CONTRATANTES** comprometem-se a observar os preceitos legais instituídos pelo ordenamento jurídico brasileiro no que tange ao combate à corrupção, em especial a Lei nº 12.846, de 1º de agosto de 2013, seus regulamentos e eventuais outras aplicáveis.

**A CONTRATADA (i)** declara, por si e por seus administradores, funcionários, representantes e outras pessoas que agem em seu nome, direta ou indiretamente, estar ciente dos dispositivos contidos na Lei nº 12.846/2013; (ii) se obriga a tomar todas as providências para fazer com que seus administradores, funcionários e representantes tomem ciência quanto ao teor da mencionada Lei nº 12.846/2013.

**A CONTRATADA** declara, com relação a este Contrato ou ao negócio dele resultante que, direta ou indiretamente, não ofereceu, prometeu, pagou ou autorizou o pagamento em dinheiro, deu ou concordou em dar presentes ou qualquer outra vantagem e, durante a vigência do contrato e a qualquer tempo, não irá ofertar, prometer, pagar ou autorizar o pagamento em dinheiro, dar ou concordar em dar presentes ou qualquer outra vantagem a qualquer pessoa ou entidade, pública ou privada, com o objetivo de beneficiar ilicitamente quaisquer das partes contratantes ou terceiros.

**PARÁGRAFO PRIMEIRO – A CONTRATADA**, no desempenho das atividades objeto deste CONTRATO, compromete-se perante à CONTRATANTE a abster-se de praticar ato(s) que possa(m) constituir violação à legislação aplicável ao presente instrumento pactual, incluindo aqueles descritos na Lei nº 12.846/2013, em especial no seu artigo 5º.

**PARÁGRAFO SEGUNDO** - Qualquer descumprimento das regras da Lei Anticorrupção e suas regulamentações, por parte da CONTRATADA, em qualquer um dos seus aspectos, poderá ensejar: I - Instauração do Procedimento de Apuração da Responsabilidade Administrativa – PAR, nos termos do Decreto nº 11.429, de 2 de março de 2023, com aplicação das sanções administrativas porventura cabíveis; II – Ajuizamento de ação com vistas à responsabilização na esfera judicial, nos termos dos artigos 18

e 19 da Lei nº 12.846/2013; III ao CONTRATANTE o direito de, agindo de boa fé, declarar rescindido imediatamente o CONTRATO, sem qualquer ônus ou penalidade, sendo a CONTRATADA responsável por eventuais perdas e danos.

**PARÁGRAFO TERCEIRO - A CONTRATADA** obriga-se a conduzir os seus negócios e práticas comerciais de forma ética e íntegra em conformidade com os preceitos legais vigentes no país.

**PARÁGRAFO QUARTO - A CONTRATADA** obriga-se a notificar prontamente, por escrito, à CONTRATANTE, a respeito de qualquer suspeita ou violação do disposto nas leis anticorrupção por meio da Ouvidoria do IFSertãoPE, através dos canais disponíveis em <https://www.ifsertao-pe.edu.br/index.php/ouvidoria>.

## 13. MODELO PADRÃO ADOTADO

Declaramos que, para a devida instrução processual, em respeito aos artigos 29 e 35 da IN nº 05/2017 e Enunciado BPC nº 06, foi utilizado o modelo de Termo de Referência constantes Templates de acordo com a IN SGD/ME nº 94, de 2022 regido pela Lei nº 14.133, de 2021 conforme o link que segue:

### Termo de Referência:

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União - CNMLC

Atualização: maio/2023

Termo de Referência contratação de Serviços TIC - Licitação

Elaborado pela Secretaria de Gestão. Complementado e Uniformizado pela CNMLC

Identidade visual pela Secretaria de Gestão

**Link:** <https://www.gov.br/agu/pt-br/composicao/cgu/cgu/modelos/licitacoescontratos/14133/modelos-da-lei-14-133-21-para-bens-e-servicos-de-tic>

## 14. NÍVEL DE ACESSO

Este documento tem nível de acesso público visto que não contém dados pessoais protegidos nem informações restritas ou sigilosas.

## 15. Responsáveis

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

**FRANCISCO HAMILTON DE FREITAS JUNIOR**

Autoridade de TIC



*Assinou eletronicamente em 20/05/2026 às 09:32:17.*

Despacho: Integrante Administrativo

**HERICA VANESSA FONSECA SILVA**

Membro da comissão de contratação

**MELQUIZEDEQUI CABRAL DOS SANTOS**

Membro da comissão de contratação

Despacho: Integrante Requisitante

**KLEMMERSON AMARIZ GOMES**

Membro da comissão de contratação

**JEAN CARLOS COELHO DE ALENCAR**

Autoridade competente



*Assinou eletronicamente em 20/05/2026 às 10:17:14.*