Ministério da Educação
Universidade Federal Rural do Semi-Árido
Pró-Reitoria de Administração
Divisão de Aquisição de Materiais e Serviços
Setor de Planejamento da Contratação

TERMO DE REFERÊNCIA N° 54/2023

(Processo Administrativo n° 23091.012197/2023-80)

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de solução de segurança e redes, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

GRUPO ÚNICO						
ITEM	**ESPECIFICAÇÃO**	**CATMAT/ CATSER**	**UNIDADE DE MEDIDA**	**QTDE**	**VL UNITÁRIO ESTIMADO**	**VL TOTAL ESTIMADO**
1	Solução de Segurança de Redes NGFW TIPO 1.	609340	und	2	R$ 670.652,69	R$ 1.341.305,39
2	Solução de Segurança de Redes NGFW TIPO 2.	609340	und	2	R$ 40.681,38	R$ 81.362,76
3	Treinamento e capacitação.	3840	UST	5	R$ 49.886,45	R$ 249.432,25
4	Suporte operacional especializado	27014	UST	40	R$ 1.555,77	R$ 62.230,67
	VALOR TOTAL ESTIMADO					**R$ 1.734.331,06**

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

1.3. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.4. O prazo de vigência da contratação é de 12 (meses) meses contados da emissão da Nota de Empenho, na forma do artigo 105 da Lei n° 14.133, de 2021.

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

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico “2 – Estimativa da Demanda - Quantidade de bens e Serviços”, especificados no Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2023, conforme detalhamento a seguir:

I) ID PCA no PNCP: 24529265000140-0-000001/2023
II) Data de publicação no PNCP: 19/05/2023
III) Id do item no PCA: 168 e 132
IV) Classe/Grupo: 111 - SERVIÇOS DE DESENVOLVIMENTO E MANUTENÇÃO DE SOFTWARE E 7050 - EQUIPAMENTOS DE REDE DE TIC - LOCAL E REMOTA
V) Identificador da Futura Contratação: 153033-45/2022 e 153033-27/2022

2.3. O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2020-2022 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2022-2026 da UFERSA, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
M1	Dar suporte ao crescimento dos serviços institucionais prestados em formato digital.

ALINHAMENTO AO PDTIC *2022-2026*			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A03	Implementação de 2 ferramentas de controle até 2026	***M03***	Gestão de identidades, monitoramento e controle de acesso às informações, recursos e serviços de TIC.
A06	Implementar 2 sistemas que dão suporte a segurança da informação até 2026	***M06***	Oferta e manutenção de infraestrutura de TIC visando aumentar a confiabilidade e a disponibilidade alinhada à expansão da Ufersa
A35	80% dos serviços digitais oferecidos pela Ufersa executados e armazenados na nuvem privada até 2026	***M35***	Atualização tecnológica e melhoria da integração dos sistemas de informação institucional (datacenter e cloud)
A36	100% dos edifícios contemplados com infraestrutura de rede	***M36***	Oferta e manutenção de infraestrutura de TIC visando aumentar a confiabilidade e a disponibilidade alinhada à expansão da Ufersa
A37	Serviços de link de internet com no mínimo 99,9% de disponibilidade		

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

3.1. SOLUÇÃO DE SEGURANÇA DE REDES NGFW

3.1.1. **SOLUÇÃO DE SEGURANÇA DE REDES NGFW TIPOS 1, 2- CARACTERISTICAS GERAIS:**

3.1.1.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux;

3.1.1.2. Poderá ser entregue em equipamento único ou com composição de equipamentos. para atender as funcionalidades exigidas;

3.1.1.3. Deverá possuir e estar licenciado pelo período de 60 (sessenta) meses para suporte, garantia, atualização de firmware e atualização automática de bases de dados, incluindo as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Otimização WAN, DLP – Data Leak Prevention, Controladora Wireless;

3.1.1.4. Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários;

3.1.1.5. Deverá incluir licença para a funcionalidade de VPN SSL;

3.1.1.6. Deverá incluir licença para atualização de vacina de antivírus/anti-spyware.

3.1.1.7. Deverá incluir licença de atualização para filtro de conteúdo Web;

3.1.1.8. Deverá incluir licença de atualização do IPS e da lista de aplicações detectadas;

3.1.1.9. Deverá possuir licença para número ilimitado de usuários e endereços IP;

3.1.1.10. Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de proteção avançada durante a vigência contratual;

3.1.1.11. Deverá possuir um relatório de uso de mídia social;

3.1.1.12. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

3.1.1.13. Deve ser compatível com os equipamentos de NGFW Fortinet FG-100F e FG-60F utilizados pela UFERSA, deve ser compatível com os softwares de gerência FortiAnalyser e o FortiManager utilizados pela UFERSA;

3.1.2. **FUNCIONALIDADES DE FIREWALL**

3.1.2.1. Deverá possuir controle de acesso à internet por endereço IP de origem e destino;

3.1.2.2. Deverá possuir controle de acesso à internet por subrede;

3.1.2.3. Deverá suportar tags de VLAN (802.1q);

3.1.2.4. Deverá possuir ferramenta de diagnóstico do tipo tcpdump;

3.1.2.5. Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

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

3.1.2.7. Deverá suportar single-sign-on para Active Directory, Novell eDirectory, Citrix e RADIUS;

3.1.2.8. Deverá possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

3.1.2.9. Deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

3.1.2.10. Deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

3.1.2.11. Deverá permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

3.1.2.12. Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

3.1.2.13. Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

3.1.2.14. Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;

3.1.2.15. Deverá suportar aplicações multimídia, como: H.323 e SIP;

3.1.2.16. Deverá possuir tecnologia de firewall do tipo Statefull;

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

3.1.2.18. Deverá permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;

3.1.2.19. Deverá suportar PBR – Policy Based Routing;

3.1.2.20. Deverá permitir a criação de VLANS no padrão IEEE 802.1q;

3.1.2.21. Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

3.1.2.22. Deverá permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

3.1.2.23. Deverá permitir forwarding de camada 2 para protocolos não IP;

3.1.2.24. Deverá suportar forwarding multicast;

3.1.2.25. Deverá suportar roteamento multicast PIM Sparse Mode e Dense Mode;

3.1.2.26. Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

3.1.2.27. Deverá permitir o agrupamento de serviços;

3.1.2.28. Deverá permitir o filtro de pacotes sem a utilização de NAT;

3.1.2.29. Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

3.1.2.30. Deverá possuir mecanismo de anti-spoofing;

3.1.2.31. Deverá permitir criação de regras definidas pelo usuário;

3.1.2.32. Deverá permitir o serviço de autenticação para tráfego HTTP e FTP;

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

3.1.2.34. Deverá possuir a funcionalidade de balanceamento e contingência de links;

3.1.2.35. Deverá suportar sFlow;

3.1.2.36. Solução deve ser capaz de prover Zero Touch provisioning.

3.1.2.37. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

3.1.2.38. O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando, ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY;

3.1.2.39. Deverá ter a capacidade de permitir a criação de regras de firewall específicas para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows;

3.1.2.40. Deverá ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

3.1.2.41. Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

3.1.2.42. Deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

3.1.2.43. Deverá suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

3.1.2.44. Deverá permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN- tagged;

3.1.2.45. Deverá possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

3.1.2.46. Deverá suportar SIP, H.323 e SCCP NAT Traversal;

3.1.2.47. Deverá permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

3.1.2.48. Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

3.1.3. **FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO**

3.1.3.1. Deverá permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

3.1.3.2. Deverá permitir modificação de valores DSCP para o DiffServ;

3.1.3.3. Deverá permitir priorização de tráfego e suportar ToS;

3.1.3.4. Deverá limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

3.1.3.5. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

3.1.3.6. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

3.1.3.7. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

3.1.3.8. Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

3.1.3.9. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

3.1.3.10. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

3.1.3.11. Deverá ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

3.1.4. **FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY**

3.1.4.1. Deverá permitir, na funcionalidade de AntiSpam, verificação do cabeçalho SMTP do tipo MIME;

3.1.4.2. Deverá possuir filtragem de e-mail por palavras chaves;

3.1.4.3. Deverá permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

3.1.4.4. Deverá possuir, para a funcionalidade de AntiSpam, o recurso de RBL;

3.1.4.5. Deverá permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

3.1.4.6. Deverá ter a capacidade de permitir a criação de perfis de AntiSpam específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs.

3.1.5. **FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**

3.1.5.1. Deverá possuir solução de filtro de conteúdo Web integrado à solução de segurança;

3.1.5.2. Deverá possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

3.1.5.3. Deverá possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;

3.1.5.4. Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;

3.1.5.5. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

3.1.5.5.1. Proxy anônimo; Webmail; Instituições de saúde; Notícias; Phishing; Hackers; Pornografia; Racismo; Websites pessoais; Compras;

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

3.1.5.7. Deverá permitir a criação de, pelo menos, 05 (cinco) categorias personalizadas;

3.1.5.8. Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

3.1.5.9. Deverá prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado;

3.1.5.10. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

3.1.5.11. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

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

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

3.1.5.14. Deverá permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;

3.1.5.15. Deverá permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

3.1.5.16. Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

3.1.5.17. Deverá permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

3.1.5.18. Deverá filtrar o conteúdo baseado em categorias em tempo real;

3.1.5.19. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

3.1.5.20. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

3.1.5.21. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

3.1.5.22. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem;

3.1.5.23. Deverá ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;

3.1.5.24. Deverá permitir o bloqueio de redirecionamento HTTP;

3.1.5.25. Deverá permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

3.1.5.26. Deverá possuir Proxy Explícito e Transparente;

3.1.5.27. Deverá implementar roteamento WCCP e ICAP;

3.1.5.28. Deverá ter a capacidade de permitir a criação de perfis de filtragem Web específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

3.1.6. **FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO**

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

3.1.6.2. Deverá possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

3.1.6.3. Deverá estar orientado à proteção de redes;

3.1.6.4. Deverá permitir funcionar em modo transparente, sniffer e router;

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

3.1.6.6. Deverá permitir a criação de padrões de ataque manualmente;

3.1.6.7. Deverá possuir integração à plataforma de segurança;

3.1.6.8. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;

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

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

3.1.6.11. Deverá possuir mecanismos de detecção/proteção de ataques;

3.1.6.12. Deverá possuir reconhecimento de padrões;

3.1.6.13. Deverá possuir análise de protocolos;

3.1.6.14. Deverá possuir detecção de anomalias;

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

3.1.6.16. Deverá possuir proteção contra-ataques de Windows ou NetBios;

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

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

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

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

3.1.6.21. Deverá possuir métodos de notificação de detecção de ataques;

3.1.6.22. Deverá possuir alarmes na console de administração;

3.1.6.23. Deverá possuir alertas via correio eletrônico;

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

3.1.6.25. Deverá ter a capacidade de resposta/logs ativa a ataques;

3.1.6.26. Deverá prover a terminação de sessões via TCP resets;

3.1.6.27. Deverá armazenar os logs de sessões;

3.1.6.28. Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

3.1.6.29. Deverá mitigar os efeitos dos ataques de negação de serviços;

3.1.6.30. Deverá permitir a criação de assinaturas personalizadas;

3.1.6.31. Deverá possuir filtros de ataques por anomalias;

3.1.6.32. Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destinationsessionlimit;

3.1.6.33. Deverá permitir filtros de anomalias de protocolos;

3.1.6.34. Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

3.1.6.35. Deverá suportar verificação de ataque na camada de aplicação;

3.1.6.36. Deverá suportar verificação de tráfego em tempo real, via aceleração de hardware;

3.1.6.37. Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset.

3.1.7. **FUNCIONALIDADE DE VPN**

3.1.7.1. Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

3.1.7.2. Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;

3.1.7.3. Deverá possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;

3.1.7.4. Deverá possuir suporte a VPN SSL;

3.1.7.5. Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

3.1.7.6. A VPN SSL deverá possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;

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

3.1.7.8. A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X;

3.1.7.9. Deverá permitir a arquitetura de VPN hub and spoke;

3.1.7.10. Deverá possuir suporte a inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

3.1.8. **FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**

3.1.8.1. Deverá reconhecer, no mínimo, 2.000 (duas mil) aplicações;

3.1.8.2. Deverá possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

3.1.8.3. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

3.1.8.4. P2P;

3.1.8.5. Transferência de arquivos;

3.1.8.6. VoIP;

3.1.8.7. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

3.1.8.8. Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

3.1.8.9. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

3.1.8.10. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

3.1.8.11. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

3.1.8.12. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

3.1.8.13. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

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

3.1.8.15. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

3.1.8.16. Deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;

3.1.8.17. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

3.1.8.18. Deverá permitir criação de padrões de aplicação manualmente;

3.1.9. **FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION)**

3.1.9.1. O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway deverá funcionar de maneira que se consiga que os dados confidenciais e ou de identificação pessoal não saiam da rede e também deverá funcionar de modo que se previna que dados não requisitados entrem na sua rede;

3.1.9.2. Deverá inspecionar, no mínimo, os tráfegos de e-mail, HTTP, NNTP e de mensageiros instantâneos;

3.1.9.3. Sobre o tráfego de e-mail, deverá inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;

3.1.9.4. Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS- Word;

3.1.9.5. Deverá fazer a varredura no conteúdo de um cookie HTTP buscando por determinado texto;

3.1.9.6. Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;

3.1.9.7. Deverá verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saintes possui um tamanho máximo especificado pelo administrador;

3.1.9.8. Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos;

3.1.9.9. Deverá tomar minimamente as ações de bloquear, banir usuário e colocar em quarentena a interface sobre as regras que coincidirem com o tráfego esperado pela regra;

3.1.9.10. Deverá permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail, HTTP e mensageiros instantâneos;

3.1.9.11. Deverá permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

3.1.10. **FUNCIONALIDADE DE BALANCEAMENTO DE CARGA**

3.1.10.1. Deverá permitir a criação de endereços IPs virtuais;

3.1.10.2. Deverá permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

3.1.10.3. Deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

3.1.10.4. Deverá permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Round Robin, Weighted, First Alive e HTTP host;

3.1.10.5. Deverá permitir persistência de sessão por cookie HTTP ou SSL session ID;

3.1.10.6. Deverá permitir que seja mantido o IP de origem;

3.1.10.7. Deverá suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

3.1.10.8. Deverá ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

3.1.10.9. Deverá permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

3.1.11. **FUNCIONALIDADE DE CONTROLADORA WIRELESS**

3.1.11.1. Deverá ser capaz de gerenciar, de forma centralizada, Pontos de Acesso do mesmo fabricante;

3.1.11.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

3.1.11.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido;

3.1.11.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;

3.1.11.5. Deverá permitir a visualização dos clientes conectados;

3.1.11.6. Deverá prover suporte a Fast Roaming;

3.1.11.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;

3.1.11.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

3.1.11.9. Deverá possuir Captive Portal por SSID;

3.1.11.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs;

3.1.11.11. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;

3.1.11.12. Deverá suportar os seguintes métodos de autenticação EAP:

3.1.11.12.1. EAP-TLS

3.1.11.12.2. EAP-TTLS;

3.1.11.12.3. EAP-PEAP;

3.1.11.12.4. EAP-SIM

3.1.11.12.5. EAP-AKA;

3.1.11.13. Deverá suportar 802.1x através de RADIUS;

3.1.11.14. Deverá suportar filtro baseado em endereço MAC por SSID;

3.1.11.15. Deverá permitir configurar parâmetros de rádio, como: banda e canal;

3.1.11.16. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

3.1.11.17. Deverá possuir mecanismo de identificação e controle de rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;

3.1.11.18. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

3.1.11.19. Deverá possuir WIDS com, ao menos, os seguintes perfis:

3.1.11.20. Rogue/Interfering AP Detection;

3.1.11.21. Ad-hoc Network Detection;

3.1.11.22. Wireless Bridge Detection;

3.1.11.23. Weak WEP Detection;

3.1.11.24. MAC OUI Checking;

3.1.11.25. Deverá permitir o uso de voz e dados sobre um mesmo SSID;

3.1.11.26. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

3.1.11.27. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário;

3.1.11.28. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs;

3.1.11.29. Deverá permitir a criação de políticas de traffic shaping;

3.1.11.30. Deverá permitir a criação de políticas de firewall baseadas em horário;

3.1.11.31. Deverá permitir NAT nas políticas de firewall;

3.1.11.32. Deverá possibilitar definir número de clientes por SSID;

3.1.11.33. Deverá permitir e/ou bloquear o tráfego entre SSIDs;

3.1.11.34. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

3.1.11.35. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;

3.1.11.36. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;

3.1.11.37. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;

3.1.11.38. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou

3.1.11.39. rádios;

3.1.11.40. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;

3.1.11.41. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;

3.1.11.42. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;

3.1.11.43. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;

3.1.11.44. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora;

3.1.11.45. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;

3.1.11.46. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

3.1.11.47. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora;

3.1.11.48. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora;

3.1.11.49. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

3.1.11.50. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora;

3.1.11.51. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora;

3.1.11.52. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede;

3.1.12. **FUNCIONALIDADE DE CONTROLADORA DE SWITCH**

3.1.12.1. Deverá ser capaz de gerenciar, de forma centralizada, Switches do mesmo fabricante;

3.1.12.2. Deve operar como ponto central para automação e gerenciamento dos switches;

3.1.12.3. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

3.1.12.4. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

3.1.12.5. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

3.1.12.6. Deve montar a topologia da rede de maneira automática;

3.1.12.7. Deve ser capaz de configurar os switches da rede;

3.1.12.8. Deve através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

3.1.12.9. Deve através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

3.1.12.10. Deve através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

3.1.12.11. Deve através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

3.1.12.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

3.1.12.13. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

3.1.12.14. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

3.1.12.15. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

3.1.12.16. Deve ser capaz de configurar parâmetros SNMP dos switches;

3.1.12.17. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

3.1.12.18. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

3.1.12.19. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches;

3.1.12.20. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

3.1.12.21. Deve prover indicadores de saúde dos elementos críticos do ambiente;

3.1.12.22. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

3.1.12.23. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

3.1.12.24. Deve possuir API no formato REST;

3.1.13. **FUNCIONALIDADE DE SD-WAN**

3.1.13.1. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

3.1.13.2. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

3.1.13.3. A solução SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

3.1.13.4. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

3.1.13.5. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

3.1.13.6. A solução deve ser capaz de criar VPN "Full-Mesh" em interface Gráfica, de forma automática, e sem que o administrador precise configurar site por site.

3.1.13.7. A configuração VPN IPSEC deverá oferecer suporte para DH Group: 14 e 15.

3.1.13.8. Reconhecimento em camada 7 totalmente segregado da camada 4.

3.1.13.9. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.

3.1.13.10. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

3.1.13.11. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc)

3.1.13.12. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6.

3.1.13.13. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.

3.1.13.14. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

3.1.13.15. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de Saúde melhor que o link atual.

3.1.13.16. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

3.1.13.17. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

3.1.14. **SOLUÇÃO DE SEGURANÇA DE REDES NGFW TIPO 1 - CARACTERISTICAS ESPECÍFICAS:**

3.1.14.1. Deverá possuir fonte de alimentação com chaveamento automático 110/220V redundante Hot Swappable. A fonte fornecida deverá suportar sozinha a operação da unidade com todos os módulos de interface ativos.

3.1.14.2. Firewall com capacidade mínima de processamento de 64 (sessenta e quatro) Gbps.

3.1.14.3. IPS com capacidade mínima de processamento de 12 (doze) Gbps.

3.1.14.4. Proteção a ameaças avançadas, isto é, com as funções de Firewall, IPS, controle de aplicação e proteção de Malware/Antivírus ativadas, com capacidade mínima de processamento de 10 (dez) Gbps. Caso o fabricante divulgue múltiplos valores para este requisito, somente o de menor valor será aceito;

3.1.14.5. Inspeção SSL Throughput com capacidade mínima de processamento de 8 (oito) Gbps.

3.1.14.6. VPN com capacidade de, pelo menos, 50 (cinquenta) Gbps de tráfego IPSec.

3.1.14.7. VPN SSL com capacidade de, pelo menos, 4 (quatro) Gbps de tráfego.

3.1.14.8. Deverá suportar 7.200.000 (sete milhões e duzentos mil) conexões simultâneas.

3.1.14.9. Deverão ser licenciados para suportar, pelo menos, 8.000 (oito mil) usuários de VPN SSL.

3.1.14.10. Deverá suportar, pelo menos, 500.000 (quinhentas mil) novas conexões por segundo.

3.1.14.11. Deverá suportar, pelo menos, 2.000 (dois mil) túneis de VPN Site-Site.

3.1.14.12. Deverá suportar, pelo menos, 40.000 (quarenta mil) túneis de VPN Client-Site.

3.1.14.13. Deverá possuir, pelo menos, 04 (quatro) interfaces SFP28 25GE.

3.1.14.14. Deverá possuir, pelo menos, 04 (quatro) interfaces SFP+ 10GE.

3.1.14.15. Deverá possuir, pelo menos, 16 (dezesseis) interfaces RJ 45.

3.1.14.16. Deverá possuir porta USB 3.0 para conexão de modem 3G/4G.

3.1.14.17. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 500 (quinhentos) Pontos de Acesso sem fio.

3.1.14.18. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 80 (oitenta) equipamentos.

3.1.15. **SOLUÇÃO DE SEGURANÇA DE REDES NGFW TIPO 2 - CARACTERISTICAS ESPECÍFICAS:**

3.1.15.1. Firewall com capacidade mínima de processamento de 6 (seis) Gbps.

3.1.15.2. IPS com capacidade mínima de processamento de 1.2 Gbps.

3.1.15.3. Proteção a ameaças avançadas, isto é, com as funções de Firewall, IPS, controle de aplicação e proteção de Malware/Antivírus ativadas, com capacidade mínima de processamento de 800 (oitocentos) Mbps. Caso o fabricante divulgue múltiplos valores para este requisito, somente o de menor valor será aceito;

3.1.15.4. Inspeção SSL Throughput com capacidade mínima de processamento de 700 (setecentos) Mbps.

3.1.15.5. VPN com capacidade de, pelo menos, 5 (cinco) Gbps de tráfego IPSec.

3.1.15.6. VPN SSL com capacidade de, pelo menos, 900 (novecentos) Mbps de tráfego.

3.1.15.7. Deverá suportar 1.200.000 (um milhão e duzentas mil) conexões simultâneas.

3.1.15.8. Deverão ser licenciados para suportar, pelo menos, 200 (duzentos) usuários de VPN SSL.

3.1.15.9. Deverá suportar, pelo menos, 40.000 (quarenta mil) novas conexões por segundo.

3.1.15.10. Deverá suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.

3.1.15.11. Deverá suportar, pelo menos, 2.000 (dois mil) túneis de VPN Client-Site.

3.1.15.12. Deverá possuir, pelo menos, 8 (oito) interfaces RJ 45.

3.1.15.13. Deverá possuir porta USB 3.0 para conexão de modem 3G/4G.

3.1.15.14. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 40 (quarenta) Pontos de Acesso sem fio.

3.1.15.15. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 15 (quinze) equipamentos.

3.2. **SERVIÇOS PROFISSIONAIS - UNIDADE DE SERVIÇOS TÉCNICOS (UST)**

3.2.1. Cada Unidade de Serviço Técnicos (UST) corresponderá à 4h (quatro horas) de profissional especializado nas plataformas ofertadas. O serviço deve ser prestado pela empresa contratada.

3.2.2. Atividades: assessement; desenvolvimento de plano de implementação; planejamento; análise; configuração; integração; migração; testes de verificação; ajustes; otimização; troubleshooting; updates; upgrades; provas de conceito; ensaios de contingência; customização de consultas de relatórios; treinamentos “hands on”; criação e manutenção de regras de segurança e redes; participação em comitês de segurança para esclarecimentos; documentação "as built"; documentação para rollout;

3.2.3. Os perfis dos profissionais/atividades definidas seguirão o padrão de perfis indicados por metodologias de projetos, como PMBOK. Abaixo, um detalhamento sobre os perfis de profissionais e o escopo de cada um de seus papeis:

3.2.4. Arquitetura: definição da arquitetura lógica e física do projeto, garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais; propor melhorias; definir controles e monitoramento do ambiente, sugerindo métricas, thresholds e indicadores de acompanhamento; apoio no planejamento, execução e avaliação de mudanças;

3.2.5. Implementação: Levantamento de dados, execução das implantações incluindo configuração customizada, integração, migrações e testes, adaptações código, criação de infraestrutura, orientação, documentação, etc;

3.2.6. Gerenciamento de projetos: gerenciamento do projeto propriamente dito, considerando controle de prazos, esforço, elaboração de relatórios de posicionamento executivo, indicadores do projeto e qualquer outra métrica prevista no PMBOOK. O objetivo de todas estas atividades é a garantia de qualidade do projeto no que tange prazos e esforço

3.2.7. Suporte: Atendimento a incidentes de suporte realizando análises, troubleshooting, diagnósticos; realizando ajustes e otimização configurações; analisando e aplicando patches, fixes e updates, aplicando testes e realizando ensaios; monitorando o ambiente;

3.2.8. As atividades deverão ser prestadas na modalidade remota;

3.2.9. **Dinâmica de contratação**

3.2.9.1. A CONTRATANTE contratará a quantidade de Unidades de Serviços Técnicos estimadas para consumo pelo período desejado durante a vigência do contrato. Emitirá nota(s) de empenho para adquirir vouchers para quantidade de Unidades de Serviços Técnicos estimados para o período correspondente.

3.2.9.2. A Contratada deve entregar os vouchers relativos à quantidade de Unidades de Serviços contratadas, que poderão ser consumidos pela CONTRATANTE ao longo do período do contrato, de acordo com a necessidade da CONTRATANTE;

3.2.9.3. A CONTRATANTE consultará a Contratada para calcular a quantidade de Unidades de Serviços Técnicos necessárias para realizar a atividade pretendida e emitirá Ordem de Serviço para a Contratada prestar os serviços. E, ao final dos serviços, contabilizará o consumo das Unidades de Serviços Técnico utilizadas;

3.2.9.4. O prazo máximo para início das atividades pela empresa contratada será de 10 (dez) dias;

3.2.9.5. As contabilizações de UST serão feitas individualmente para cada profissional alocado;

3.2.9.6. As UST executadas fora do expediente comercial por solicitação deste órgão, serão contabilizadas em dobro;

3.2.9.7. A empresa Contratada deve nomear funcionário capacitado que será responsável por fornecer aconselhamento técnico e operacional sobre os serviços; assistência sobre as condições do contrato; gerenciamento de escalação junto ao Fabricante; Gerenciamento de recursos e cronograma de entrega dos serviços;

3.2.9.8. Neste modelo de execução dos serviços não se caracteriza a subordinação direta e nem a pessoalidade, visto que não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da empresa contratada e este Órgão. As empresas proponentes deverão considerar em seus custos todos os recursos necessários ao completo atendimento aos objetos, tais como despesas com pessoal (salários, férias, encargos, benefícios, seleção, outras) de modo a garantir os serviços definidos;

3.2.9.9. Para o controle da execução dos serviços será utilizado a Unidade de medida UST (Unidade de Serviço Técnico). A UST consiste na "moeda" usada para dimensionar todas as atividades que serão demandadas pela CONTRATANTE, no escopo de cada Ordem de Serviço. A contratação será em volume de UST por atividade e a licitação resultará na oferta do valor de uma UST que irá representar o esforço combinado de profissionais envolvidos, variando a complexidade e prioridade da atividade.;

3.3. **TREINAMENTO OFICIAL**

3.3.1. O treinamento deverá ser do tipo oficial do fabricante da solução ofertada;

3.3.2. Deverá ser realizado para uma turma de até 5 alunos;

3.3.3. Deverá ser ministrado por instrutor capacitado;

3.3.4. Deverá ocorrer no formato presencial;

3.3.5. Deverá ser realizado em datas previamente agendadas entre a CONTRATANTE e CONTRATADA;

3.3.6. Deverá ocorrer em dias úteis, dentro do horário comercial;

3.3.7. O treinamento deverá ser realizado contemplando uma das tecnologias contidas na solução ofertada, a ser previamente combinado entre a CONTRATANTE e CONTRATADA;

3.3.8. Deverá estar incluso voucher para realização da prova de certificação oficial do fabricante para 5 alunos.

3.3.9. Deverá estar incluso transporte para cidade onde será realizado o treinamento e hospedagem na cidade onde será realizado o treinamento para 5 pessoas.

3.3.10. O treinamento deve ser executado em centro de treinamento oficial do fabricante

4. REQUISITOS DA CONTRATAÇÃO

Sustentabilidade:

4.1. 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:

4.1.1. Só será admitida a oferta de bens de informática e/ou automação que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs).

Indicação de marcas ou modelos

4.2. Na presente contratação será admitida a indicação da(s) seguinte(s) marca(s), característica(s) ou modelo(s), de acordo com as justificativas contidas nos Estudos Técnicos Preliminares: FortiAnalyser; FortiManager; FortiGate; FortiAP.

a) em decorrência da necessidade de padronização do objeto;

b) em decorrência da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração;

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

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

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

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

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

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

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

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

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

5.2. São obrigações do CONTRATADO:

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

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

5.2.3. reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato 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, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso;

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

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

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

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

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

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

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

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

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

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

6. MODELO DE EXECUÇÃO DO OBJETO

Condições de Entrega

6.1. O prazo de entrega dos bens é de 90 dias, contados da finalização do processo licitatório, em remessa única.

6.2. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 30 dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

6.3. Os bens deverão ser entregues no seguinte endereço: Av. Francisco Mota, 572 - Bairro Costa e Silva, Mossoró RN | CEP: 59.625-900.

Garantia, manutenção e assistência técnica

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

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

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

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

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

6.9. Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 05 (cinco) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

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

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

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

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

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 a contratada 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.

7.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de

fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

7.6. 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).

7.7. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

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

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

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

7.7.4. 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).

7.7.5. O fiscal técnico do contrato comunicar 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).

7.8. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

7.8.1. Caso ocorram 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).

7.9. O gestor do contrato 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).

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

7.9.2. 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).

7.9.3. 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).

7.9.4. 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).

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

7.11. O gestor do contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

8. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

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

8.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 30(trinta) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

8.3. O recebimento definitivo ocorrerá no prazo de 15(quinze) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

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

8.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

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

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

8.8. 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.

Liquidação

8.9. 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.

8.9.1. 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.

8.10. 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:

a) o prazo de validade;
b) a data da emissão;
c) os dados do contrato e do órgão contratante;
d) o período respectivo de execução do contrato;
e) o valor a pagar; e
f) eventual destaque do valor de retenções tributárias cabíveis.

8.11. 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;

8.12. 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.

8.13. 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.

8.14. 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.

8.15. 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.

8.16. 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.

8.17. 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

8.18. 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.

8.19. 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 Índice de Custo da Tecnologia da Informação (ICTI*)* de correção monetária.

Forma de pagamento

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

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

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

8.22.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.23. 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

8.24. 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.

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

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

8.26. 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, tudo nos termos do Parecer JL-01, de 18 de maio de 2020.

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

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

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.

Exigências de habilitação

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

Habilitação jurídica

9.3. **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;

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

9.5. **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;

9.6. **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;

9.7. **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.

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

9.9. **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

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

9.11. **Agricultor familiar:** Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pela Secretaria Especial de Agricultura Familiar e do Desenvolvimento Agrário, nos termos do art. 4º, §2º do Decreto nº 10.880, de 2 de dezembro de 2021.

9.12. **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).

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

Habilitação fiscal, social e trabalhista

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

9.15. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

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

9.17. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

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

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

9.20. Caso o fornecedor seja considerado isento dos tributos 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.

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

Qualificação Econômico-Financeira

9.22. 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;

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

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

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

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

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

9.25. 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 capital mínimo ou patrimônio líquido mínimo de 10%(dez por cento) do valor total estimado da contratação

9.26. 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).

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

9.28. *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

9.29. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

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

9.29.2. Fornecimento de um mínimo de 01 unidade de appliance de Next Generation Firewall de mesmo porte ou superior

9.29.3. Fornecimento de serviço especializado em administração e ou suporte em Next Generation firewall com um mínimo de 80 horas

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

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

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

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

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

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

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

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

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

9.30.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

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

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. O custo estimado médio total da contratação é de R$ R$ 1.734.331,06 (um milhão, setecentos e trinta e quatro mil, trezentos e trinta e um reais e seis centavos).

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. Por se tratar de Sistema de Registro de Preços, a indicação da dotação orçamentária fica postergada para o momento da assinatura do contrato ou instrumento equivalente.