CONSELHO REGIONAL DE MEDICINA DO ESTADO DO CEARÁ

TERMO DE REFERÊNCIA (TR)

Minuta para contratação de serviços TIC não continuado e continuado / Licitação ou contratação direta sem RP

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

Modelo de Termo de Referência – Aquisições – Licitação e Contratação Direta - Lei nº 14.133, de 2021

Aprovado pela Secretaria de Gestão e Inovação

Atualização: SET/2025

Adaptado

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de serviço de uso de ***Next Generation Firewall (NGFW)*** físico, com em regime de comodato, com funcionalidade de ***SD-WAN***, pelo período de 12 (doze) meses, serviço de implantação e migração da solução atual, garantia e suporte do fabricante com direito de atualização do produto durante a vigência do contrato, para a sede do CREMEC, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Prestação de serviço de uso d e ***Next Generation Firewall (NGFW)*** físico com funcionalidade d e ***SD-WAN***, pelo período de 12 (doze) meses, serviço de implantação e migração da solução atual, garantia e suporte do fabricante com direito de atualização do produto durante a vigência do contrato	609340	meses	12 (doze)	R$2.216,67	R$ 26.600,00

Classificação do objeto quanto à heterogeneidade ou complexidade

1.2. O serviço objeto desta contratação é caracterizado como **comum**.

Classificação do objeto quanto ao modelo de execução

1.3. O serviço é enquadrado como **continuado** tendo em vista que, embora o TCU e a Lei nº 14.133, de 2021, admitam fixação de prazo inicial de vigência superior a 12 (doze) meses, é vantajoso para a Administração manter o prazo inicial de vigência de 12 (doze) meses considerando a natureza da contratação e práticas do mercado.

Prazo de vigência

1.4. O prazo de vigência da contratação é de **12 (doze) meses** contados da **assinatura do contrato**, na forma do art. 105 da Lei nº 14.133, de 2021.

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

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A presente contratação justifica-se para garantir a confiabilidade e segurança da informação que transitará pela rede do CREMEC, assim como sua integridade, confidencialidade, autenticidade e disponibilidade de acesso, de forma a garantir a preservação e segurança da informação que, hoje, é considerada um dos ativos mais valiosos, não só pela sua importância estratégica, mas também por ser um elemento de fundamental importância para tomada de decisões pelas instituições e órgãos públicos.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2026, conforme consta das informações básicas desse Termo de Referência.

2.3. Nos termos do art. 14, inciso I, da Instrução Normativa SEGES/ME nº 58/2022, o Estudo Técnico Preliminar (ETP) é formalmente dispensado nas hipóteses de contratação direta fundamentadas no art. 75, inciso II, da Lei nº 14.133/2021, em razão do baixo valor da contratação. No presente caso, o valor estimado da contratação enquadra-se na referida hipótese legal de dispensa de licitação por valor, razão pela qual não foi elaborado ETP em documento apartado. Todavia, considerando tratar-se de contratação de solução de Tecnologia da Informação e Comunicação (TIC), em respeito as diretrizes da IN SGD nº 94/2022, que exigem a realização de planejamento técnico da contratação, esses elementos encontram-se incorporados a este Termo de Referência.

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

3.1. A solução de TIC consiste em *Appliance de Next Generation Firewall (NGFW).*

3.2. Características:

3.2.1. 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.

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

3.2.3. Deverá possuir e estar licenciado pelo período de 60 (sessenta) meses com 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 e Virtualização.

3.2.4. Firewall com capacidade mínima de processamento de 8 (oito) Gbps.

3.2.5. IPS com capacidade mínima de processamento de 1 (um) Gbps.

3.2.6. 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 700 (setecentos) Mbps.

3.2.7. Inspeção SSL Throughput com capacidade mínima de processamento de 500 (quinhentos) Mbps.

3.2.8. VPN com capacidade de, pelo menos, 6 (seis) Gbps de tráfego IPSec.

3.2.9. VPN SSL com capacidade de, pelo menos, 800 (oitocentos) Mbps de tráfego.

3.2.10. Deverá suportar 600.000 (seiscentas mil) conexões simultâneas.

3.2.11. Deverão ser licenciados para suportar, pelo menos, 150 (cento e cinquenta) usuários de
VPN SSL.

3.2.12. Deverá suportar, pelo menos, 30.000 (trinta mil) novas conexões por segundo.

3.2.13. Deverá suportar, pelo menos, 150 (cento e cinquenta) túneis de VPN Site-Site.

3.2.14. Deverá suportar, pelo menos, 400 (quatrocentos) túneis de VPN Client-Site.

3.2.15. Deverá possuir, pelo menos, 8 (oito) interfaces RJ45.

3.2.16. Todos os equipamentos que acompanharem a solução deverão suportar operação em modo de alta disponibilidade e estar licenciados para operar desta forma.

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

3.2.18. 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.

3.2.19. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 30 (trinta) Pontos de Acesso sem fio.

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

3.2.21. Deverá ser compatível e Gerenciado pelo item “Dispositivo de Gerência Centralizada de Dispositivos de Segurança Redes”.

3.2.22. Deverá ser compatível com o item “Dispositivo Gerência Centralizada para Coleta, Armazenamento e Análises de Log”.

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

3.2.24. Deverá incluir licença para a funcionalidade de VPN SSL

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

3.2.26. Deverá incluir licença de atualização para filtro de conteúdo Web.

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

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

3.2.29. REQUISITOS GERAIS DE FUNCIONALIDADES E LICENCIAMENTOS PARA FIREWALL

3.2.29.1. FUNCIONALIDADES DE FIREWALL

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

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

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

3.2.29.1.4. Deverá possuir ferramenta de diagnóstico do tipo tcpdump;

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

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

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

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

3.2.29.1.9. 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;

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

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

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

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

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

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

3.2.29.1.16. 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;

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

3.2.29.1.18. Deverá suportar PBR – Policy Based Routing;

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

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

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

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

3.2.29.1.23.Deverá suportar forwarding multicast;

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

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

3.2.29.1.26.Deverá permitir o agrupamento de serviços;

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

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

3.2.29.1.29.Deverá possuir mecanismo de anti-spoofing;

3.2.29.1.30.Deverá permitir criação de regras definidas pelo usuário;

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

3.2.29.1.32.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;

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

3.2.29.1.34.Deverá suportar sFlow;

3.2.29.1.35.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;

3.2.29.1.36.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;

3.2.29.1.37.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;

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

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

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

3.2.29.1.41.Deverá permitir funcionamento em modo bridge, router, proxy explícito, sniffere/ou VLAN- tagged;

3.2.29.1.42.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;

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

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

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

3.2.30. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

3.2.30.1. 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;

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

3.2.30.3. Deverá permitir priorização de tráfego e suportar ToS;

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

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

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

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

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

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

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

3.2.30.11. 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.

3.2.31. FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

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

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

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

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

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

3.2.31.6. 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, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

3.2.32. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

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

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

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

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

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

3.2.32.6. Proxy anônimo;

3.2.32.7. Webmail;

3.2.32.8. Instituições de saúde;

3.2.32.9. Notícias;

3.2.32.10. Phishing;

3.2.32.11. Hackers;

3.2.32.12. Pornografia;

3.2.32.13. Racismo;

3.2.32.14. Websites pessoais;

3.2.32.15. Compras;

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

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

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

3.2.32.19. 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;

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

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

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

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

3.2.32.24. 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;

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

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

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

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

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

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

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

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

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

3.2.32.34. Deverá permitir o bloqueio de redirecionamento HTTP;

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

3.2.32.36. Deverá possuir Proxy Explícito e Transparente;

3.2.32.37. Deverá implementar roteamento WCCP e ICAP;

3.2.32.38. 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.

3.2.33. FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

3.2.33.1. 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;

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

3.2.33.3. Deverá estar orientado à proteção de redes;

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

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

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

3.2.33.7. Deverá possuir integração à plataforma de segurança;

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

3.2.33.9. 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;

3.2.33.10. 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;

3.2.33.11. Deverá ter a capacidade de permitir a criação de perfis de inspeção 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;

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

3.2.33.13. Deverá possuir reconhecimento de padrões;

3.2.33.14. Deverá possuir análise de protocolos;

3.2.33.15. Deverá possuir detecção de anomalias;

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

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

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

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

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

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

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

3.2.33.23. Deverá possuir alarmes na console de administração;

3.2.33.24. Deverá possuir alertas via correio eletrônico;

3.2.33.25. 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;

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

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

3.2.33.28. Deverá armazenar os logs de sessões;

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

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

3.2.33.31. Deverá permitir a criação de assinaturas personalizadas;

3.2.33.32. Deverá possuir filtros de ataques por anomalias;

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

3.2.33.34. Deverá permitir filtros de anomalias de protocolos;

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

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

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

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

3.2.34. FUNCIONALIDADE DE VPN

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

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

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

3.2.34.4. Deverá possuir suporte a VPN SSL;

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

3.2.34.6. 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;

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

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

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

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

3.2.34.11. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

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

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

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

3.2.34.15. P2P;

3.2.34.16. Instant Messaging;

3.2.34.17. Web;

3.2.34.18. Transferência de arquivos;

3.2.34.19. VoIP;

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

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

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

3.2.34.23. Deverá prover funcionalidade de identificação transparente de

usuários cadastrados no Microsoft Active Directory;

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

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

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

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

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

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

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

3.2.34.31. Deverá permitir criação de padrões de aplicação manualmente;

3.2.34.32. Deverá ter a capacidade de permitir a criação de perfis de controle de aplicações 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.

3.2.35. FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION)

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

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

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

3.2.35.4. Sobre o tráfego de mensageiros instantâneos, deverá inspecionar, os protocolos atualmente em uso;

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

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

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

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

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

3.2.35.10. 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;

3.2.35.11. 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;

3.2.35.12. 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.

3.2.36. FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

3.2.36.1. Deverá permitir a criação de endereços IPs virtuais;

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

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

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

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

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

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

3.2.36.8. 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;

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

3.2.37. FUNCIONALIDADE DE VIRTUALIZAÇÃO

3.2.37.1. Deverá suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

3.2.37.2. Deverá permitir a criação de administradores independentes para cada uma das instâncias virtuais;

3.2.37.3. Deverá permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

3.2.38. FUNCIONALIDADE DE CONTROLADORA WIRELESS E WI-FI

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

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

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

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

3.2.38.5. Deverá permitir a visualização dos clientes conectados;

3.2.38.6. Deverá prover suporte a Fast Roaming;

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

3.2.38.8. 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;

3.2.38.9. Deverá possuir Captive Portal por SSID;

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

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

3.2.38.12. Deverá suportar os seguintes métodos de autenticação EAP:

3.2.38.13. EAP-TTLS;

3.2.38.14. EAP-PEAP;

3.2.38.15. EAP-SIM

3.2.38.16. EAP-AKA;

3.2.38.17. Deverá suportar 802.1x através de RADIUS;

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

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

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

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

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

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

3.2.38.24. Rogue/Interfering AP Detection;

3.2.38.25. Ad-hoc Network Detection;

3.2.38.26. Wireless Bridge Detection;

3.2.38.27. Weak WEP Detection;

3.2.38.28. MAC OUI Checking;"

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

3.2.38.30. 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;

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

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

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

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

3.2.38.35. Deverá permitir NAT nas políticas de firewall;

3.2.38.36. Deverá possibilitar definir número de clientes por SSID;

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

3.2.38.38. 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;

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

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

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

3.2.38.42. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios;

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

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

3.2.38.45. 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;

3.2.38.46. 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;

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

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

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

3.2.38.50. 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;

3.2.38.51. 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;

3.2.38.52. 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;

3.2.38.53. Deverá permitir aplicar políticas de controle AntiSpam para todas as

redes cujo tráfego seja tunelado até a Controladora;

3.2.38.54. 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;

3.2.38.55. 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;

3.2.38.56. Deverá possuir as seguintes certificações:

3.2.38.57. Certificação Wi-Fi Alliance;

3.2.38.58. Certificação ICSA para Firewall;

3.2.38.59. Certificação ICSA para Antivírus;

3.2.38.60. Certificação ICSA para VPN SSL;

3.2.38.61. Certificação ICSA para VPN IPSec;

3.2.38.62. Certificação ICSA para IPS;"

3.2.38.63. O equipamento de firewall e/ou IPS deverá ter sido aprovado nos testes da NSS Labs e deverá estar na lista de recomendados.

3.2.39. FUNCIONALIDADE DE SD-WAN

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

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

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

3.2.39.4. 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.

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

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

3.2.39.7. 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.

3.2.39.8. 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.

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

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

3.2.39.11. 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.

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

3.2.39.13. 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)

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

3.2.39.15. 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.

3.2.39.16. 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.

3.2.39.17. 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.

3.2.39.18. 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.

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

3.3. GARANTIA, SUPORTE E LICENCIAMENTO

3.3.1. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de 36 meses;

3.3.2. A garantia deverá ser de 12 meses;

3.3.3. Deve contemplar suporte do Fabricante pelo período vigente, com no mínimo, as seguintes características:

3.3.4. O suporte do fabricante/contratada deve ter um sistema de abertura de chamados para acompanhamento – funcionando 24 horas por dia e 7 dias por semana. Para atendimento telefônico, deve operar em língua Portuguesa pelo menos em regime 8x5;

3.3.5. Deve assegurar a utilização de novas versões de software da solução sem ônus a Licitante, sempre que esta estiver disponível a qualquer cliente;

3.3.6. Deve permitir o acesso à base de conhecimento da solução;

3.4. Serviço de Instalação

3.4.1. Planejamento

3.4.1.1. Reunião inicial com o cliente para levantamento de dados e pré-requisitos necessários para implantação dos equipamentos;

3.4.1.2. Discussão do cenário para seguir as melhores práticas de redundância e compliance;

3.4.1.3. Elaboração da planilha onde contém todos os dados necessário

para implementação e validado pelo cliente.

3.4.2. Instalação remota

3.4.2.1. Instalação remota dos equipamentos adquiridos com auxílio da TI local;

3.4.2.2. Acompanhar a conectorização dos cabos nos equipamentos ofertados seguindo as melhores práticas e planejamento.

3.4.3. Appliance de Segurança

3.4.3.1. Associação das licenças adquiridas;

3.4.3.2. Inicialização básica seguindo o planejamento;

3.4.3.3. Atualização de Firmware para a versão mais recente suportada;

3.4.3.4. Configuração de Alta Disponibilidade (HA) quando necessário;

3.4.3.5. Configuração de SD-WAN para balanceamento de links WAN, MPLS, VPN quando necessário;

3.4.3.6. Configuração da autenticação 802.1x

3.4.3.7. Criação de serviços DHCP para redes controladas pelo appliance quando necessário;

3.4.3.8. Configuração das interfaces físicas e/ ou virtuais para segregação de rede;

3.4.3.9. Integração com servidor LDAP para autenticações;

3.4.3.10. Integração com Active Directory para autenticação do tipo SSO quando necessário;

3.4.3.11. Gerenciamento autenticado com usuários LDAP;

3.4.3.12. Instalação de até 1 certificado digital quando necessário;

3.4.3.13. Configuração para inspeção de tráfego SSL;

3.4.3.14. Configurações de túneis e conexões IPSEC e SSL VPN;

3.4.3.15. Configuração de grupos de usuários para navegação por perfil;

3.4.3.16. Configuração de proteção anti-malware;

3.4.3.17. Configurações de controle de aplicação de acordo com perfil de grupo de usuários;

3.4.3.18. Configurações de Web Filter, IPS e Traffic Shapping;

3.4.3.19. Criação de até 15 políticas de Firewall;

3.4.3.20. Configuração de Logs.

3.4.4. Documentação e Repasse de Conhecimento

3.4.4.1. Toda implementação será no formato remoto ;

3.4.4.2. Relatório de implementação;

3.4.4.3. Overview do ambiente ao final da implementação.

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio:

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

4.1.1. Garantir a confidencialidade, integridade, autenticidade e disponibilidade das informações que trafegam pela rede do CREMEC, protegendo-as contra acessos não autorizados, ataques cibernéticos e vazamento de dados;

4.1.2. Assegurar a continuidade operacional dos serviços de TI do CREMEC mediante solução de segurança de rede de alto desempenho, com funcionalidades integradas de NGFW, SD-WAN, IPS, Antivírus, Filtro Web, VPN e DLP;

4.1.3. Substituir e migrar a solução de firewall atualmente em operação, garantindo a manutenção das políticas de segurança vigentes e sem interrupção dos serviços institucionais.

Requisitos de Capacitação

4.2. Faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto. O treinamento deverá abranger as funcionalidades do appliance NGFW contratado, incluindo configuração, monitoramento, análise de logs e resolução de incidentes, sendo realizado de forma remota, conforme previsto no item de Documentação e Repasse de Conhecimento do presente TR.

Requisitos Legais

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

Requisitos de Manutenção

4.4. Devido às características da solução, há necessidade de realização de manutenções **corretivas, preventivas e evolutivas** pela Contratada, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades, incluindo:

4.4.1. Atualização de firmware para a versão mais recente suportada durante toda a vigência contratual;

4.4.2. Atualização automática das bases de dados de proteção avançada (antivírus, IPS, filtro de conteúdo web e controle de aplicações);

4.4.3. Manutenção corretiva mediante abertura de chamados no portal de atendimento da Contratada, observando os prazos definidos na Tabela de Níveis Mínimos de Serviço (Anexo I deste TR).

Requisitos Temporais

4.5. Os serviços devem ser prestados no prazo máximo de ***10 (dez)*** dias corridos, a contar da assinatura do contrato, emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

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

4.7. Todos os prazos citados, quando não expresso de forma contrária, serão

considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

4.8. Na execução dos serviços de suporte, deverão ser observados os seguintes prazos, conforme nível de severidade do chamado:

Severidade	Descrição	Prazo Máximo de Solução
1 – ALTA	Solução totalmente indisponível ou grande degradação	6 horas corridas
2 – MÉDIA	Solução parcialmente indisponível ou com perda de funcionalidades	12 horas corridas
3 – BAIXA	Solução disponível com ocorrência de alarmes ou pouco impacto	Até o 2º dia útil
4 – CONSULTORIA	Atividades de consultoria, dúvidas e ajustes não urgentes	Até o 5º dia útil

Requisitos de Segurança e Privacidade

4.9. A solução deverá atender aos princípios e procedimentos da Política de Segurança da Informação do CREMEC, em conformidade com a LGPD (Lei nº 13.709/2018).

Requisitos Sociais, Ambientais e Culturais

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

4.10.1. Preferência, quando disponível no mercado, por fabricantes ou soluções que adotem práticas de responsabilidade socioambiental em sua cadeia produtiva;

4.10.2. A solução ofertada deverá estar em conformidade com as diretrizes do Guia Nacional de Contratações Sustentáveis da AGU, no que for aplicável à contratação de serviços de TIC.

Regime de disponibilização do equipamento

4.11. O appliance NGFW será disponibilizado pela Contratada em regime de comodato, durante toda a vigência contratual, sem transferência de propriedade à Contratante. Ao término do contrato, e não havendo prorrogação ou nova contratação que justifique sua permanência, o equipamento deverá ser recolhido pela Contratada, sem ônus adicional para a Contratante, observados os procedimentos de transição e finalização contratual.

Requisitos da Arquitetura Tecnológica

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

4.13. Os equipamentos fornecidos deverão ser novos, originais de fábrica (não podem ter sido recondicionados), de primeiro uso, da geração na respectiva linha de produtos do fabricante.

4.14. Os equipamentos deverão ser idênticos aos da proposta comercial da contratação;

4.15. As soluções de gerenciamento centralizado e a solução de gerência e armazenamento de logs deverão ser do mesmo fabricante dos equipamentos de NGFW ofertados;

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

Requisitos de Projeto, de Implementação e de Implantação

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

4.17.1. Elaboração de planilha de implementação validada pelo cliente;

4.17.2. Instalação remota dos equipamentos com auxílio da TI local;

4.17.3. Configuração de Alta Disponibilidade (HA), SD-WAN, autenticação 802.1x, interfaces físicas/virtuais, LDAP/Active Directory (SSO), inspeção SSL, túneis VPN IPSec/SSL, perfis de usuários, anti-malware, Web Filter, IPS, Traffic Shaping e até 15 políticas de Firewall;

4.17.4. Entrega de relatório de implementação e overview do ambiente ao final.

Requisitos de Garantia e Manutenção

4.18. O prazo de garantia contratual dos equipamentos e serviços será de, no mínimo, 12 (doze) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto, complementar à garantia legal.

4.19. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de 36 (trinta e seis) meses.

4.20. O suporte do fabricante/contratada deverá operar 24 horas por dia, 7 dias por semana para abertura de chamados, e atendimento telefônico em língua portuguesa em regime mínimo de 8x5.

Requisitos de Experiência Profissional

4.21. Os serviços de assistência técnica, suporte e garantia deverão ser prestados por técnicos devidamente certificados nos produtos ofertados, com todos os recursos ferramentais necessários para a prestação dos serviços.

Requisitos de Formação da Equipe

4.22. Os serviços de assistência técnica, suporte e garantia deverão ser prestados por técnicos devidamente identificados e pertencentes ao quadro de

funcionários da empresa contratada.

Requisitos de Metodologia de Trabalho

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

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

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

Requisitos de Segurança da Informação e Privacidade

4.26. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos neste instrumento, em especial:

4.26.1. Sigilo e confidencialidade sobre todas as informações da infraestrutura de rede e dados do CREMEC acessadas durante a execução dos serviços;

4.26.2. Conformidade com a LGPD (Lei nº 13.709/2018) no tratamento de quaisquer dados pessoais eventualmente acessados durante a vigência contratual;

4.26.3. Vedação ao uso, reprodução ou divulgação das informações do CREMEC para fins alheios ao objeto contratual.

Vistoria

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

Indicação de marcas ou modelos

4.28. Na presente contratação será indicada a seguinte marca/modelo como referência: **Fortigate 60F** .

Subcontratação

4.29. Não será admitida a subcontratação do objeto contratual.

Garantia da contratação

4.30. Não haverá exigência da garantia da contratação dos art. 96 e seguintes da Lei nº 14.133, de 2021, pela natureza do objeto.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

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

5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço

ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

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

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

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

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

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

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

5.2. São obrigações do CONTRATADO:

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

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

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

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

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

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

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

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

5.2.9. fazer a transição contratual, quando for o caso.

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

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

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

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

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

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

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

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

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

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

6. MODELO DE EXECUÇÃO DO OBJETO

Condições de execução

6.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1. Início da execução do objeto: *10* dias *da assinatura do contrato*.

Local e horário da prestação dos serviços

6.2. Os serviços serão prestados no seguinte endereço: Av. Antônio Sales, nº 485, Joaquim Távora, Fortaleza/CE, CEP 60.135-101;

6.3. Os serviços serão prestados no seguinte horário: *08h à 17h.*

Rotinas a serem cumpridas

6.4. A execução contratual observará as rotina s *já previstas neste instrumento.*

Materiais a serem disponibilizados

6.5. Para a perfeita execução dos serviços, o Contratado deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades, promovendo sua substituição quando necessário.

Formas de transferência de conhecimento

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

Procedimentos de transição e finalização do contrato

6.7. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas(IN – Seges/MP 5/2017):

6.7.1. a adequação dos recursos materiais e humanos necessários à continuidade do serviço por parte da Administração;

6.7.2. a transferência final de conhecimentos sobre a execução e a manutenção do serviço, incluindo a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução dos serviços;

6.7.3. a devolução ao órgão ou entidade dos equipamentos, espaço físico, crachás, dentre outros;

6.7.4. cessão ao contratante de todos os direitos patrimoniais relativos ao objeto contratado;

6.7.5. no caso de contratações de TIC, entrega das versões finais dos produtos e da documentação;

6.7.6. devolução ao contratante dos recursos de sua propriedade, tais como: equipamentos, mobiliário, espaço físico, entre outros;

6.7.7. liberação à CONTRATADA da garantia contratual, descontadas eventuais multas devidas ao contratante, além de obrigações trabalhistas e previdenciárias não pagas;

6.7.8. liberação à CONTRATADA do saldo remanescente dos recursos depositados na Conta-Depósito Vinculada, quando aplicável, após a comprovação da quitação de todos os encargos trabalhistas e previdenciários relativos ao serviço contratado;

6.7.9. outras providências que se apliquem: revogar perfis de acesso, recolher crachás, trocar senhas que porventura sejam de conhecimento dos empregados da CONTRATADA, eliminar caixas postais.

Quantidade mínima de serviços para comparação e controle

6.8. Cada OS conterá o volume de serviços demandados, incluindo a sua localização e o prazo.

Mecanismos formais de comunicação

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

I - Ordem de Serviço;

II - Ata de Reunião;

III - Ofício;

IV - Sistema de abertura de chamados;

V - E-mails e Cartas;

VI - Aplicativos de conversa.

Manutenção de Sigilo e Normas de Segurança

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

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.

Preposto

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

7.6. O Contratado **não necessitará** manter preposto da empresa no local da execução do objeto.

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

Reunião Inicial

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

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

7.10. A pauta desta reunião observará, pelo menos:

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

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

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

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

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

Rotinas de Fiscalização

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

Fiscalização Técnica

7.12. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.13. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

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

7.15. O fiscal técnico do contrato informará ao gestor do 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.

7.16. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

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

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

Fiscalização Administrativa

7.19. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias,

as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.20. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

7.21. O fiscal do contrato enviará a documentação pertinente ao Setor de Contabilidade para a formalização dos procedimentos de liquidação e pagamento, com a indicação expressa de que o valor da Nota Fiscal emitida pela contratada confere com o valor dimensionado pela fiscalização no recebimento definitivo do serviço.

Gestor do Contrato

7.22. Cabe ao gestor do contrato:

7.22.1. coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

7.22.2. acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

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

7.22.4. emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.22.5. tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

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

7.22.7. acompanhar o envio da documentação pelos fiscais do contrato para a formalização dos procedimentos de liquidação e pagamento, com conferência do valor da Nota Fiscal emitida pela contratada.

7.22.8. receber e dar encaminhamento imediato:

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

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

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. A avaliação da execução do objeto utilizará os NÍVEIS MÍNIMOS DE SERVIÇO (NMS), conforme o disposto nesta seção.

Classificação de Severidade dos Chamados

Nível	Severidade	Descrição da Ocorrência	Prazo de 1º Atendimento	Prazo de Solução
1	**CRÍTICA**	Solução totalmente indisponível ou com grande degradação que impede o funcionamento da rede	Até **1 hora** corrida	Até **6 horas** corridas
2	**ALTA**	Solução parcialmente indisponível ou com perda significativa de funcionalidades (ex.: IPS, VPN, filtro web fora de operação)	Até **2 horas** corridas	Até **12 horas** corridas
3	**MÉDIA**	Solução disponível com degradação de desempenho, geração de alarmes ou perda de funcionalidades não críticas	Até **4 horas** comerciais	Até **2 dias úteis**
4	**BAIXA**	Solução plenamente disponível; chamado de consultoria, dúvidas técnicas ou solicitações de ajustes de configuração	Até **8 horas** comerciais	Até **5 dias úteis**

Disponibilidade Mínima Exigida

Parâmetro	Índice Exigido	Período de Medição
Disponibilidade da solução NGFW	≥ **99,5%**	Mensal
Janela de manutenção programada	Até **4 horas/mês** (fora do horário comercial, com aviso prévio de 48h)	Mensal
Tempo máximo de indisponibilidade acumulada (Severidade 1)	≤ **3,6 horas/mês**	Mensal

Penalidades por Descumprimento dos NMS

Situação de Descumprimento	Desconto na Fatura Mensal
Não solução de chamado **Severidade 1** no prazo	**2%** por hora de atraso, limitado a **10%** do valor mensal
Não solução de chamado **Severidade 2** no prazo	**1%** por hora de atraso, limitado a **5%** do valor mensal
Não solução de chamado **Severidade 3 ou 4** no prazo	**0,5%** por dia de atraso, limitado a **3%** do valor mensal

Critérios de Medição e Faturamento

Item	Critério
Unidade de medição	Mês de serviço prestado
Período de medição	Do 1º ao último dia do mês de referência
Instrumento de medição	Relatório mensal de chamados extraído do portal de atendimento da Contratada, validado pelo fiscal técnico do contrato
Prazo para apresentação da NF	Até o **5º dia útil** do mês subsequente ao da prestação do serviço

Item	Critério
Prazo para pagamento	Até **30 dias** após o atestado do fiscal, conforme art. 141 da Lei nº 14.133/2021
Forma de pagamento	Mensal, proporcional ao período de efetiva prestação do serviço

Cálculo da Disponibilidade

A disponibilidade mensal será apurada pela seguinte fórmula:

$$D(\%) = \frac{T_{total} - T_{indisp}}{T_{total}} \times 100$$

Onde:

T_{total} = Total de horas do período de medição (horas corridas no mês);

T_{indisp} = Somatório das horas de indisponibilidade não programada registradas no período, excluídas as janelas de manutenção previamente acordadas.

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

8.2.1. não produziu os resultados acordados,

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

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

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

Recebimento

8.4. Os serviços serão recebidos provisoriamente, no prazo de *05 (cinco)* dias, pelo fiscal, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

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

8.6. 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.

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.

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, será considerado para fins de faturamento o período mensal.

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

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

8.11. 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.

8.12. 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.

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

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

8.15. 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.

8.16. 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.

8.17. Os serviços serão recebidos definitivamente no prazo de **10 (dez) 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:

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

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

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

8.17.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o

valor exato dimensionado pela fiscalização.

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

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

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

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

Procedimentos de Teste e Inspeção

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

8.21.1. Aspectos físicos e documentais do appliance entregue;

8.21.2. Concluída a implantação pela Contratada, o fiscal técnico realizará ou acompanhará a execução dos seguintes testes de desempenho e conectividade; e

8.21.3. O fiscal técnico verificará, mediante acesso supervisionado à console de administração do appliance, se as funcionalidades estão devidamente configuradas e estão operacionais.

Liquidação

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

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

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

I - o prazo de validade;

II - a data da emissão;

III - os dados do contrato e do órgão contratante;

IV - o período respectivo de execução do contrato;

V - o valor a pagar; e

VI - eventual destaque do valor de retenções tributárias cabíveis.

8.25. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que

impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante.

8.26. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

8.27. A Administração deverá realizar consulta ao SICAF para:

8.27.1. verificar a manutenção das condições de habilitação exigidas;

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

8.28. 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.

8.29. 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.

8.30. 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.

8.31. 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

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

Forma de pagamento

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

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

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

8.35.1. 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.

8.36. 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.

Reajuste

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

8.38. Após o interregno de um ano, e condicionado à solicitação da Contratada, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, acumulado no período de doze meses anteriores à data da pesquisa de preços, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

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

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

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

8.43. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

8.44. O reajuste será realizado por apostilamento.

Cessão de Crédito

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

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

8.45.2. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

8.45.3. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de

direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

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

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

9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO

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

Ocorrência	Descrição	Tipo
Atraso na implantação e migração da solução	Não conclusão dos serviços de instalação remota, configuração e migração no prazo de 30 dias corridos previsto na Ordem de Serviço	Mora
Não atendimento de chamado de Severidade 1 (Crítica) no prazo	Não registro de 1º atendimento no prazo de 1 hora corrida ou não solução em 6 horas corridas	Inexecução Parcial
Não atendimento de chamado de Severidade 2 (Alta) no prazo	Não registro de 1º atendimento no prazo de 2 horas corridas ou não solução em 12 horas corridas	Inexecução Parcial
Não atendimento de chamado de Severidade 3 (Média) no prazo	Não solução de chamado de média criticidade em até 2 dias úteis	Inexecução Parcial
Não atendimento de chamado de Severidade 4 (Baixa/Consultoria) no prazo	Não solução de chamado de baixa criticidade em até 5 dias úteis	Inexecução Parcial
Falha na atualização automática das bases de proteção	Não atualização automática das bases de IPS, Antivírus e/ou Filtro de Conteúdo Web, comprometendo a proteção da rede do CREMEC	Inexecução Parcial

Ocorrência	Descrição	Tipo
Não entrega ou entrega incompleta da documentação técnica	Ausência de relatório de implementação, planilha de dados validada, overview do ambiente ou manual do equipamento no prazo acordado	Mora
Não realização da capacitação técnica no prazo acordado	Não realização do repasse de conhecimento à equipe de TI do CREMEC sobre as funcionalidades do NGFW contratado	Mora
Substituição de equipamento por modelo inferior ao contratado	Entrega de appliance diferente do modelo aprovado na proposta ou com especificações inferiores às exigidas no TR	Inexecução Total
Não manutenção das licenças ativas durante a vigência contratual	Interrupção ou expiração antecipada do licenciamento de NGFW, IPS, Antivírus, Filtro Web, VPN SSL, DLP ou SD-WAN	Inexecução Parcial
Descontinuidade no suporte 24x7 para abertura de chamados	Portal de atendimento indisponível para abertura/acompanhamento de chamados por mais de 4 horas consecutivas	Inexecução Parcial
Não fornecimento de suporte telefônico em língua portuguesa (8x5)	Ausência de atendimento telefônico em português durante o horário comercial (8h às 17h, dias úteis)	Inexecução Parcial
Recusa injustificada em realizar testes de aceite	Recusa ou impedimento à realização dos testes funcionais e de configuração previstos nos Procedimentos de Teste e Inspeção (item 8.22)	Inexecução Parcial
Quebra de sigilo e confidencialidade das informações do CREMEC	Divulgação, reprodução ou uso indevido de dados, topologia de rede ou informações institucionais do CREMEC por parte da Contratada	Inexecução Total

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

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

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

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

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

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

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

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

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

9.4.4. Multa:

9.4.4.1. Moratória, para as infrações descritas no item “d”, de **0,5%** (**cinco décimos** por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de **15** (**quinze**) dias.

9.4.4.2. Compensatória, para as infrações descritas acima alíneas “**e**” a “**h**” de **10**% (**dez** por cento) a **30**% (**trinta** por cento) do valor da contratação.

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

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

9.4.4.5. Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de **8**% (**oito** por cento) a **15**% (**quinze** por cento) do valor da contratação.

9.4.4.6. Compensatória, para a infração descrita acima na alínea “**a**”, de **0,5%** (**cinco décimos** por cento) a **2**% (**dois** por cento) do valor da contratação.

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

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

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

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

9.9. A multa poderá ser recolhida administrativamente no prazo máximo de *10* (*dez*) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

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

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

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

9.11. Na aplicação das sanções serão considerados:

9.11.1. a natureza e a gravidade da infração cometida;

9.11.2. as peculiaridades do caso concreto;

9.11.3. as circunstâncias agravantes ou atenuantes;

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

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

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

9.13. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar

confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

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

9.14.1. As penalidades serão obrigatoriamente registradas no SICAF.

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

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

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

Forma de seleção e critério de julgamento da proposta

10.1. O fornecedor será selecionado por meio de contratação direta com fundamento no art. **75**, inciso **II**, da Lei nº 14.133, de 2021, com base no valor estimado da contratação.

Exigências de habilitação

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

Habilitação jurídica

10.3. 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;

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

10.5. 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;

10.6. 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;

10.7. 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.

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

10.9. 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;

10.10. 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.

10.11. Consórcio de empresas: contrato de consórcio devidamente arquivado no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis (art. 279 da Lei nº 6.404, de 15 de dezembro de 1976) ou compromisso público ou particular de constituição, subscrito pelos consorciados, com a indicação da empresa líder, responsável por sua representação perante a Administração (art. 15, caput, I e II, da Lei nº 14.133, de 2021).

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

Habilitação fiscal, social e trabalhista

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

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

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

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

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

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

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

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

Qualificação Econômico-Financeira

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

10.22. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

Qualificação Técnica

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

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

Qualificação Técnico-Operacional

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

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

10.24.1.1. contrato(s) que comprove(m) a experiência mínima de 01 (um) ano do fornecedor na prestação dos serviços, em períodos sucessivos ou não, sendo aceito o somatório de atestados de períodos diferentes;

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

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

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

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

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

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

Disposições gerais sobre habilitação

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

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

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

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

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

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação, que é o máximo aceitável, é de R$ 26.800,00 (vinte e seis mil e oitocentos reais), conforme custos unitários apostos na **tabela:**

Produto/serviço	Unidade	Valor unitário	Valor Total
NGFW + Licenciamento	12 meses	R$ 1.800,00	R$ 21.800,00
Instalação e configuração de appliance NGFW e treinamento da equipe local	1	R$ 5.000,00	R$ 5.000,00

11.2. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

11.3. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre Contratante e Contratado.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no orçamento do CREMEC.

12.2. A dotação relativa aos exercícios financeiros subsequentes será indicada no início de cada exercício e liberação dos créditos correspondentes, mediante apostilamento.

13. DISPOSIÇÕES FINAIS

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

Fortaleza, na data da assinatura eletrônica.

RAUL GABIEL CARVALHO DE MELO

RAIMUNDO MIRANDA RIBEIRO DA SILVA

Área de TIC

DRA. INÊS TAVARES VALE E MELO

Presidente do Conselho Regional de Medicina do Estado do Ceará – CREMEC

ANEXO I – NÍVEIS MÍNIMOS DE SERVIÇO Nível Mínimo de Serviço (NMS)

O Nível Mínimo de Serviço define os termos e as condições sob as quais a CONTRATADA deverá prover o serviço de firewall com a garantia e suporte elencadas no Termo de Referência; O serviço de garantia e suporte técnico deverá ser prestado, remotamente quando possível e pessoalmente, quando necessário, nos locais de instalação dos equipamentos.

Deverá ser disponibilizado no portal de atendimento área de consulta do chamado, incluindo hora de abertura e fechamento assim como o andamento deste.

As informações sobre os chamados deverão permanecer armazenadas até o final do contrato, sendo possível acessá-las através do portal de atendimento por qualquer usuário da CONTRATANTE na solução; A CONTRATADA deverá cumprir prazos máximos para resposta aos acionamentos (Tabela 1), de acordo com o nível de severidade de cada chamado:

Severidade ALTA: Esse nível de severidade é aplicado quando a solução se encontra totalmente indisponível ou funcionando de forma intermitente ou grande degradação de performance. Há uma falha nos componentes da solução que deixem indisponíveis

seus recursos. Há impacto a todos os usuários.

Severidade MÉDIA: Esse nível de severidade é aplicado quando há falha, simultânea ou não, do uso da solução, em que se encontra parcialmente indisponível ou com degradação de performance ou perda de funcionalidades e serviços que afetem grande parte dos usuários;

Severidade BAIXA: Esse nível de severidade é aplicado quando a solução se encontra disponível, mas há ocorrência de alarmes, ou com pouco impacto a um ou mais usuários. Também quando for necessário realizar consulta sobre problemas ou dúvidas gerais sobre a solução, manutenções preventivas e corretivas não urgentes, atualizações de softwares, firmwares, reconfiguração de ambiente, ou ajustes não urgentes e necessários na solução para seu perfeito funcionamento.

Severidade CONSULTORIA: Todas as atividades de consultoria

Severidade	**Descrição**	**Prazo Máximo de Solução**
1 – ALTA	Solução totalmente indisponível ou grande degradação	6 horas corridas
2 – MÉDIA	Solução parcialmente indisponível ou com perda de funcionalidades	12 horas corridas
3 – BAIXA	Solução disponível com ocorrência de alarmes ou pouco impacto	Até o 2º dia útil
4 – CONSULTORIA	Atividades de consultoria, dúvidas e ajustes não urgentes	Até o 5º dia útil

Documento assinado eletronicamente por **Raul Gabriel Carvalho de Melo**, **Analista de Sistemas**, em 24/04/2026, às 10:33, com fundamento no art. 5º da RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022.

Documento assinado eletronicamente por **Raimundo Miranda Ribeiro da Silva**, **Técnico de Informática**, em 24/04/2026, às 11:19, com fundamento no art. 5º da RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022.

A autenticidade do documento pode ser conferida no site https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4117326** e o código CRC **B969312D**.