PREFEITURA MUNICIPAL DE MONTENEGRO

TERMO DE REFERÊNCIA

CAPÍTULO I
DA DEFINIÇÃO DO OBJETO

1. OBJETO

O presente Termo de Referência tem por objetivo determinar as condições que disciplinarão a contratação dos serviços de (solução integrada de segurança da informação, incluindo firewall do tipo Next Generation, licenças de proteção para endpoints e servidores, sistema de inventário e acesso remoto, mitigação de ataques DDoS, além de suporte técnico contínuo e treinamento para a equipe de TI da Prefeitura Municipal de Montenegro), de acordo com o Estudo Técnico Preliminar e conforme condições, quantidades, exigências e estimativas contidas neste Termo de Referência.

Lote	Item	Unidade de Medida	Qtde	Descritivo	Valor Unitário de Referência	Valor Total de Referência	Exclusividade ME/EPP
1	1	Mês	60	Locação de serviço de solução integrada Next Generation I composta de 2 equipamentos (appliance = hardware + software) de segurança da informação, com licenças e suporte técnico 24x7.	R$ 16.700,11	R$ 1.002.006,60	Não
	2	Mês	60	Locação de serviço de solução integrada Next Generation II composta de 2 equipamentos (appliance = hardware + software) de segurança da informação, com licenças e suporte técnico 24x7.	R$ 7.950,00	R$ 477.000,00	
	3	Mês	60	Disponibilização de licenças para 880 desktops para uso de solução corporativa de proteção e segurança com gerência em nuvem e com suporte técnico 24x7.	R$ 33.150,30	R$ 1.989.018,00	
	4	Mês	60	Disponibilização de licenças para 20 servidores para uso de solução corporativa de proteção e segurança com gerência em nuvem e com suporte técnico 24x7.	R$ 3.835,77	R$ 230.146,20	
	5	Mês	60	Disponibilização de licenças para 880 dispositivos, capaz de efetuar acesso remoto, gestão de ativos e inventário com gerência em nuvem e com suporte técnico 24x7.	R$ 13.250,35	R$ 795.021,00	
	6	Mês	60	Disponibilização solução de mitigação de ataque DDoS e CDN com gerência em nuvem e com suporte técnico 24x7.	R$ 816,67	R$ 49.000,20	

PREFEITURA MUNICIPAL DE MONTENEGRO

	7	Unidade	1	Serviço de Instalação dos itens 1 a 6	R$ 61.366,67	R$ 61.366,67	
	8	Unidade	1	Treinamento das soluções	R$ 28.890,00	R$ 28.890,00	

1.1. DESCRIÇÃO DO ITEM 1 – LOCAÇÃO DE EQUIPAMENTO NEXT GENERATION

1.1.1. Deverá ser entregue dois equipamentos idênticos para atender a funcionalidade de cluster do tipo HA;
1.1.2 O equipamento deve ser instalado e configurado em rack com largura padrão, padrão EIA-310, ocupando no máximo 1U (44,45 mm) do referido rack; O equipamento poderá ser reinstalado em rack em outro local (entenda-se sala ou prédio) por parte da contratada sempre que existir a necessidade da parte da **Prefeitura Municipal de Montenegro**.
1.1.3 Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;
1.1.4 Possuir painel ou led indicador on/off e devices de rede;
1.1.5 Possuir throughput de no mínimo 57 Gbps para tráfego bruto;
1.1.6 Suportar no mínimo 12.800.000 (doze milhões e oitocentos mil) conexões simultâneas;
1.1.7 Suportar no mínimo 230.000 (duzentos e trinta mil) novas conexões por segundo;
1.1.8 Possuir throughput mínimo de 4.9 Gbps para tráfego IPS/IDS;
1.1.9 Possuir throughput mínimo de 30 Gbps para tráfego VPN IPSEC;
1.1.10 Possuir estrutura voltada para appliance de segurança, não sendo aceito soluções OEM ou servidores de mercado montados e destinados para segurança. A fabricante do software deverá ser a mesma fabricante da solução de hardware.
1.1.11 Possuir pelo menos 12 (doze) interfaces de rede gigabit ethernet com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
1.1.12 Possuir no mínimo 4portas SFP+(10G);
1.1.13 Possuir no mínimo 3portas USB;
1.1.14 Possuir dispositivo de armazenamento interno de no mínimo 180 GB padrão SSD;
1.1.15 Possuir no mínimo 1 (uma) porta console de conexão para acesso à interface de comando CLI específica para esta finalidade;
1.1.16 Possuir pelo menos 1 (uma) porta de dedicado gerenciamento.

1.2 DESCRIÇÃO DO ITEM 2 – LOCAÇÃO DE EQUIAPMENTO NEXT GENERATION

1.2.1 Deverá ser entregue dois equipamentos idênticos para atender a funcionalidade de cluster do tipo HA.
1.2.2 O equipamento deve ser instalado e configurado em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45 mm) do referido rack; O equipamento poderá ser reinstalado em rack em outro local (entenda-se sala ou prédio) por parte da contratada sempre que existir a necessidade da parte da Prefeitura Municipal de Montenegro.

1.2.3 Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;
1.2.4 Possuir painel ou led indicador on/off e devices de rede;
1.2.5 Possuir throughput de no mínimo 29 Gbps para tráfego UDP;
1.2.6 Suportar no mínimo 6.300.000 (seis milhões trezentas mil) conexões simultâneas;
1.2.7 Suportar no mínimo 55.000 (cinquenta e cinco mil) novas conexões por segundo;
1.2.8 Possuir throughput mínimo de 2.5 Gbps para tráfego IPS/IDS;
1.2.9 Possuir throughput mínimo de 11 Gbps para tráfego VPN IPSEC;
1.2.10 Possuir estrutura voltada para appliance de segurança, não sendo aceito soluções OEM ou servidores de mercado montados e destinados para segurança. A fabricante do software deverá ser a mesma fabricante da solução de hardware.
1.2.11 Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
1.2.12 Possuir no mínimo 2 portas SFP;
1.2.13 Possuir dispositivo de armazenamento interno de no mínimo 80 GB padrão SSD;
1.2.14 Possuir no mínimo 1 (uma) porta console de conexão para acesso a interface de comando CLI específica para esta finalidade;
1.2.15 Possuir pelo menos 1 (uma) porta de dedicado gerenciamento;

1.3 RESUMO PARA OS ITENS 1 E 2

1.3.1 FUNÇÕES BÁSICAS

1.3.1.1 Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;
1.3.1.2 VPN SSL, VPN ipsec (Client-to-site e Site-to-site);
1.3.1.3 Controle de Aplicações;
1.3.1.4 Proxy Web e Filtro de Conteúdo Web (URL Filtering);
1.3.1.5 Detecção e prevenção de intrusos – IPS;
1.3.1.6 Qualidade de serviço – QOS;
1.3.1.7 Anti-Malware;
1.3.1.8 SD-WAN;
1.3.1.9 Cluster.
1.3.1.10 Controle de ameaças

1.3.2 FUNÇÔES BASICAS DE SEGURANÇA

1.3.2.1 Appliance voltado a proteção de redes e internet, efetuando a proteção perimetral e de rede interna que inclui stateful para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QOS), VPN IPSEC e SSL, IPS, prevenção contra ameaças de vírus, malwares, filtro de URL, controle de ameaças por DNS, cloud sandbox, inspeção de tráfego criptografado e proteção de aplicação Web. Deverão ser fornecidas todas as licenças para atualização de todos os componentes de software, vacinas de malwares, assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de aplicação web pelo período mínimo de 24 (vinte e quatro) meses.
1.3.2.2 Os equipamentos deverão ser configurados desde o primeiro instante em modo HA (ativo-passivo) ou HA (ativo-ativo).
1.3.2.3 Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos novos, sem uso anterior.

1.3.2.4 Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.
1.3.2.5 Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.
1.3.2.6 Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.
1.3.2.7 O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Caso ocorra o fim de suporte da solução inicialmente ofertada, caberá a contratada a total substituição da solução antes do termino de suporte, sem custos adicionais, durante a vigência contratual.
1.3.2.8 Interface em português e inglês;
1.3.2.9 O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;
1.3.2.10 Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.
1.3.2.11. A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho.
1.3.2.12. Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;
1.3.2.13. Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;

1.3.3. SEGURANÇA EMBARCADA

1.3.3.1. Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;
1.3.3.2. Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;
1.3.3.3. Deve possuir ferramentas para realizar backups de forma remota, por SSH, FTP, NFS ou próprio do fabricante. Deve também permitir backup em Pendrive. A solução deve permitir o agendamento diário ou semanal do backup;
1.3.3.4. Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.
1.3.3.5. Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica;
1.3.3.6. As cópias de segurança devem ser salvas criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;
1.3.3.7. Deve permitir habilitar ou desabilitar o registro de log por política da solução.
1.3.3.8. Possuir controle de acesso à internet por endereço IP de origem e destino;
1.3.3.9. Possuir controle de acesso à internet por sub-rede;
1.3.3.10. Possuir suporte a tags de VLAN (802.1q);
1.3.3.11. Suportar agregação de links, segundo padrão IEEE 802.3ad;
1.3.3.12. Possuir ferramenta de diagnóstico do tipo pcap;
1.3.3.13. Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;
1.3.3.14. Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

1.3.3.15. Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.
1.3.3.16. Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
1.3.3.17. Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;
1.3.3.18. Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
1.3.3.19. Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;
1.3.3.20. Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
1.3.3.21. Deverá suportar aplicações multimídia como: H.323, SIP;
1.3.3.22. Possuir tecnologia de varredura do tipo Stateful;
1.3.3.23. Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo/passivo e ativo/ativo;
1.3.3.24. Permitir o funcionamento em modo transparente tipo “bridge”;
1.3.3.25. Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;
1.3.3.26. Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);
1.3.3.27. Deverá suportar forwarding de multicast;
1.3.3.28. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP e UDP;
1.3.3.29. Permitir o agrupamento de serviços;
1.3.3.30. Permitir o filtro de pacotes sem a utilização de NAT;
1.3.3.31. Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
1.3.3.32. Possuir mecanismo de anti-spoofing;
1.3.3.33. Permitir criação de regras definidas pelo usuário;
1.3.3.34. Permitir o serviço de autenticação para HTTP e FTP;
1.3.3.35. Possuir a funcionalidade de balanceamento e contingência de links;
1.3.3.36. Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: WhatsAppWeb, Yahoo! Mail Messenger, skype, ICQ, Facebook Messenger, entre outros.

1.3.4. RECONHECIMENTO DE LOGINS

1.3.4.1. Deve possuir a capacidade de criação de políticas de acesso ao equipamento, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;
1.3.4.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
1.3.4.3. Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;
1.3.4.4. A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;
1.3.4.5. Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;
1.3.4.6. A solução de identificação de usuário deverá se integrar com as funcionalidades de segurança, controle de aplicação e IPS, sendo elas do mesmo fabricante;

1.3.5. CONEXÃO SEGURA

1.3.5.1. VPN baseada em appliance;
1.3.5.2. Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
1.3.5.3. Suporte a certificados PKI X.509 para construção de vpns;
1.3.5.4. Possuir suporte a vpn sipsec site-to-site:
1.3.5.5. Criptografia, 3DES, AES128, AES256, AES-GCM-128
1.3.5.6. Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
1.3.5.7. Algoritmo Internet Key Exchange (IKE) versões I e II;
1.3.5.8. AES 128 e 256 (Advanced Encryption Standard);
1.3.5.9. Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14;
1.3.5.10. Possuir suporte a VPN SSL;
1.3.5.11. Possuir capacidade de realizar SSL vpns utilizando certificados digitais;
1.3.5.12. Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços RDP, VNC, SSH, WEB e SMB.
1.3.5.13. Deve permitir a arquitetura de vpn hub andspoke;
1.3.5.14. Suporte a vpn sipsec client-to-site;
1.3.5.15. Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.
1.3.5.16. Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);
1.3.5.17. Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).

1.3.6. GESTÃO DE AMEÇAS

1.3.6.1. A Detecção de Intrusão deverá ser baseada em appliance;
1.3.6.2. Possuir no mínimo 7.000 assinaturas ou regras de IPS/IDS;
1.3.6.3. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
1.3.6.4. Possuir tecnologia de detecção baseada em assinatura;
1.3.6.5. Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass;
1.3.6.6. O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;
1.3.6.7. Possuir opção para administrar as listas de Blacklist, Whitelist e Quarentena com suporte a endereços ipv6;
1.3.6.8. 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;
1.3.6.9. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denialof Service (dos) do tipo Flood, Prot Scan e Sweep;
1.3.6.10. Mecanismos de detecção/proteção de ataques;
1.3.6.11. Reconhecimento de padrões;
1.3.6.12. Análise de protocolos;
1.3.6.13. Detecção de anomalias;
1.3.6.14. Detecção de ataques de RPC (Remote procedure call);
1.3.6.15. Proteção contra ataques de Windows ou netbios;

1.3.6.16. Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
1.3.6.17. Proteção contra ataques DNS (Domain Name System);
1.3.6.18. Proteção contra ataques a FTP, SSH, Telnet e rlogin;
1.3.6.19. Proteção contra ataques de ICMP (Internet Control Message Protocol);
1.3.6.20. Alertas via correio eletrônico;
1.3.6.21. Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
1.3.6.22. Capacidade de resposta ativa a ataques;
1.3.6.23. Terminação de sessões via TCP resets;
1.3.6.24. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
1.3.6.25. O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
1.3.6.26. Possuir filtros de ataques por anomalias;
1.3.6.27. Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
1.3.6.28. Permitir filtros de anomalias de protocolos;
1.3.6.29. Suportar reconhecimento ou suprimir ataques de DoS;
1.3.6.30. Suportar verificação de ataque nas camadas de aplicação;

1.3.7. PRIORIDADE DE TRAFEGO

1.3.7.1. Adotar solução de Qualidade de Serviço baseada em appliance;
1.3.7.2. 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;
1.3.7.3. Permitir modificação de valores DSCP;
1.3.7.4. Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;
1.3.7.5. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
1.3.7.6. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
1.3.7.8. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active
1.3.7.9. Directory e LDAP;
1.3.7.10. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
1.3.7.11. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

1.3.8. VARREDURA DE AMEÇAS

1.3.8.1. Possuir funções de detecção de ameaças com mecanismo duplo de varredura eAnti-spyware;
1.3.8.2. Possuir scan em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS e FTP;
1.3.8.3. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);
1.3.8.4. Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

1.3.9. CONTROLE WEB

1.3.9.1. Possuir solução de filtro de conteúdo web integrado a solução de segurança;
1.3.9.2. Possuir pelo menos 85 categorias para classificação de sites web;
1.3.9.3. Possuir base mínima contendo, 1 milhão de sites internet web já registrados e classificados;
1.3.9.4. Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:
Webmail/Web-based Email; Instituições de Saúde/Saúde e bem-estar; Notícias; Pornografia; Restaurante; Mídias Sociais; Esporte; Educação; Games; Compras;
1.3.9.5. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
1.3.9.6. Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;
1.3.9.7. Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;
1.3.9.8. Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;
1.3.9.9. Possibilitar a integração com servidores de cache WEB externos;
1.3.9.10. Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update;
1.3.9.11. Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;
Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
1.3.9.12. Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
1.3.9.13. Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
1.3.9.14. 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, activex através de: base de URL própria atualizável;
1.3.9.15. Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
1.3.9.16. Permitir a criação de listas personalizadas de urls permitidas – lista branca e bloqueadas – lista negra;
1.3.9.17. Deverá permitir o bloqueio de urls inválidas cujo campo CN do certificado SSL não contém um domínio válido;
1.3.9.18. Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
1.3.9.19. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
1.3.9.20. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
1.3.9.21. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
1.3.9.22. Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
1.3.9.23. Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de áudio, vídeo e urls originadas de Spam;
1.3.9.24. Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS e FTP;
1.3.9.25. Deverá permitir configurar a porta do Proxy;

1.3.10. VARREDURA DE APLICAÇÕES

1.3.10.1. As funcionalidades abaixo devem ser baseadas em Appliance:

1.3.10.2. Reconhecer pelo menos 3.500 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado à peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, voip, streaming de mídia/vídeo ou áudio, proxy ou tunelamento, mensagens instantâneas ou colaboração, compartilhamento de arquivos/storage, backup, mail;
1.3.10.3. Reconhecer pelo menos as seguintes aplicações: 4Shared, Active Directory/SMB, Citrix ICA, DHCP protocol;
1.3.10.4. Dropbox Download, Easy Proxy, Facebook, Firefox Update, Freegate, Gmail, logmein, NTP, RPC over HTTP, Skype, SNMP Trap, anydesk, teamviewer, TOR, P2P, Ultrasurf, VNC, whatsapp, whatsapp File Transfer e whatsapp Web; controlar aplicações baseadas em categorias, característica (Ex: Banda e produtividade consumida), tecnologia (Ex: P2P) e risco;
1.3.10.5. Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook, Freegate Proxy/Searching, Google Drive , Google Plus, Facebook (Applications, Chat, Like Button/Plugin, Message/Messenger, Plugin(s), Posting, Messenger VoipCall/Videochat Chat, Vídeo Playback), Freegate Proxy/Searching, Gmail (Attachment), Google Drive (File Download, File Upload), Google Earth Application, Google Plus, linkedin, Twitter (Message,), Yahoo (Mail/webmail, File Attach) e Youtube (Vídeo Search, video Streaming/Play, Upload);
1.3.10.6. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
1.3.10.7. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, porthopping e túnel através de tráfego SSL encriptado;
1.3.10.8. Atualizar a base de assinaturas de aplicações automaticamente;
1.3.10.9. Reconhecer aplicações em ipv6;
1.3.10.10. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
1.3.10.11. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
1.3.10.12. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
1.3.10.13. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
1.3.10.14. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
1.3.10.15. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
1.3.10.16. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
1.3.10.17. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

1.3.11. MECANISMO AVANÇADO DE AMEAÇAS

1.3.11.1. Possuir sistema de proteção avançada contra ameaças (ATP) nativo;
1.3.11.2. O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios;
1.3.11.3. Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;

1.3.11.4. A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;
1.3.11.5. Deve permitir a identificação de aplicativos e ameaças independente das portas e protocolos;
1.3.11.6. Possuir mecanismo de bloqueio para listas de reputação de endereço IP catalogadas no mínimo para 6(seis) categorias, capaz de permitir seleção por categorização, elas devem atender às seguintes classificações: spam, reputation, malware, attacks, anonymous e abuse;
1.3.11.7. Deve permitir a atualização automática das assinaturas por meio de agendamento diário;
1.3.11.8. Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, ataques P2P, trojans, worms, malwares para mobile, blacklist, vulnerabilidades conhecidas;
1.3.11.9. Possuir varredura de ameças não conhecidas por meio de envio de amostra a cloud do fabricante, tipo Sandbox;
1.3.11.10. Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, ataques P2P, trojans, worms, malwares para mobile, blacklist, vulnerabilidades conhecidas;
1.3.11.11. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de voip tais como: Hotline, SIP, Skype;
1.3.11.12. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Badoo, Airtime, Blogger, Facebook, Flickr, FC2, Google Analytics, ICQ, Linkdin, Meetup, Skype, Tinder, Tuenti, Twitter, whatsapp, wechat e Zoho Chat;
1.3.11.13. Possuir capacidade de utilizar-se de informações (hostname e ip) de ferramentas de segurança de terceiros, voltadas ao registro de endereços atacantes, que enviam spam e efetuam ataques, dessa forma a unidade fará a coleta sistemática desses endereços e utilizará como forma de bloquear acessos oriundos desses endereços já catalogados por outras ferramentas de segurança;
1.3.11.14. Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;
1.3.11.15. Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;
1.3.11.16. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as “ameaças detectadas” e as “ameaças bloqueadas”;
1.3.11.17. Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os “aplicativos detectados” e os “aplicativos bloqueados”;
1.3.11.18. Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: “baixo; médio e alto”;
1.3.11.19. Gerar registro do tipo Top Level, dos 10 (dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados.

1.3.12. GERENCIAMENTO DE CONEXÃO

1.3.12.1. Entende-se como tecnologia SD-WAN (Software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de qos, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos;
1.3.12.2. Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;
1.3.12.3. Permitir utilizar VPN ipsec para interligar unidades remotas;
1.3.12.4. Possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link;
1.3.12.5. O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;

1.3.12.6. Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos relacionado ao recurso SD-WAN;
1.3.12.7. Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações:
1.3.12.8. Consumo de banda; Perda de pacotes; Jitter; Latência.

1.3.13. CLUSTER

1.3.13.1. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Passivo ou Ativo/Ativo, com as implementações de Fail Over;
1.3.13.2 Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador;
1.3.13.3 O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat.

1.3.14. CONTROLE DE MULTIPLOS LINKS

1.3.14.1. A solução proposta deve suportar o balanceamento de carga e redundância para pelo menos 2 (dois) links de Internet;
1.3.14.2. A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação;
1.3.14.3. A solução proposta deve fornecer opções de condições em caso de falha “Failover” do link de Internet através dos protocolos ICMP, TCP e UDP;
1.3.14.4. A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway;
1.3.14.5. A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego ipv4 e ipv6.

1.3.15. GERENCIAMENTO, DASHBOARD E RELATÓRIOS

1.3.15.1. A solução proposta deve permitir que todos os appliances armazenem seus relatórios internamente conforme espaço disponível interno na própria unidade.
1.3.15.2. Permitir a customização dos relatórios padrão da solução, permitindo o administrador criar relatórios de acordo com as necessidades do ambiente e informações desejadas.
1.3.15.3. Permitir que o administrador realize agendamentos destes relatórios para que estes sejam enviados via e-mail para todos os emails cadastrados.
1.3.15.4. A solução de segurança deverá ser entregue com redundância de armazenamento, na console de gestão em cloud, deverá a proponente disponibilizar solução com pelo menos 500 de armazenamento em nuvem (por unidade de cluster), devidamente licitando para tal atividade.
1.3.15.5. Armazenar histórico dos relatórios em disco local e/ou em cloud.
1.3.15.6. Possuir relatórios únicos para cada um dos módulos ofertados pela solução.
1.3.15.7. Possuir multiformato de relatórios, pelo menos tabular e gráfico.
1.3.15.8. Permitir exportar relatórios para: PDF, CSV.
1.3.15.9. Possuir relatórios sobre as pesquisas realizadas pelos usuários nos principais buscadores: Yahoo, Bing e Google.
1.3.15.10. Possuir relatórios que informem principais atividades em cada módulo.
1.3.15.11. Ter logs em tempo real.
1.3.15.12. Ter logs arquivados para consulta posterior.
1.3.15.13. Permitir que o administrador consiga realizar pesquisas dentro dos logs arquivados.
1.3.15.14. Possuir logs de auditoria.

1.3.15.15. Ter sua gerência totalmente baseada em acesso web.
1.3.15.16. Permitir que o administrador crie regras baseadas em usuários onde cada usuário criado poderá ter acesso a funcionalidades específicas na ferramenta.
1.3.15.17. O administrador deve poder acessar estes relatórios de qualquer lugar através de apenas um navegador.
1.3.15.18. Ter total gerencia sobre a retenção dos dados armazenados nos equipamentos.
1.3.15.19. Ter disponibilidade de envio de logs externo.

1.3.16. DO SUPORTE TÉCNICO 24X7

1.3.16.1. Serviço de suporte REMOTO para os equipamentos de segurança de borda contratados, no horário 24x7 (Todos os dias da semana e todos os meses do ano, inclusive feriados), pelo tempo de contrato, com as seguintes características:
1.3.16.2. A contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativo aos equipamentos e/ou produtos fornecidos;
1.3.16.3. Todos chamados de recursos, suporte, ativações devem ser catalogados na ferramenta de tickets/helpdesk da contratada, sendo necessário sempre o envio de e-mails com as ações realizadas;
1.3.16.4. A contratada deverá iniciar o atendimento de suporte remoto em no máximo 4 horas úteis após a abertura do chamado e solução do problema em até 12 horas;
1.3.16.5. Atendimentos que necessitem deslocamento técnico deverão ser atendidos em no máximo oito (8) horas após abertura do chamado por profissional legalmente empregado da empresa vencedora do edital;
1.3.16.6. Em caso de defeito do equipamento a troca deve ser efetuada em no máximo 12 horas após abertura do chamado, no endereço instalado;
1.3.16.7. A contratada poderá ser acionada para quaisquer ajustes, atualizações, configurações ou ativação de recursos enquanto estiver no período contratual, sem custos adicionais a contratante. O atendimento poderá ser realizado presencial caso o ajuste em questão necessite de intervenção local;
1.3.16.8. Quando ocorrer o lançamento de novas versões de firmwares, o licenciamento do produto deverá permitir o acesso sem custo adicional as mais novas versões dos softwares;
1.3.16.9. Quando da necessidade de aplicação de patch e firmwares, esses deverão ser instalados pela contratada durante período oposto ao turno de trabalho da prefeitura. Somente será autorizado atualizações com o respectivo aviso a equipe técnica desta Prefeitura.
1.3.16.10. Caso o a solução apresente defeito durante o contrato, caberá a contratada a substituição da unidade, incluindo custos de transporte deslocamento e reinstalação se for necessário.
1.3.16.11. A contratada será responsável pela retenção e realização dos backups dos dispositivos instalados.
1.3.16.12. No decorrer do contrato, caso a fabricante indique que a solução inicialmente ofertada entrou em End-of-Support ou termino de suporte ou atualização, caberá a contratada fornecer solução do mesmo fabricante e de mesmo porte para a substituição da solução, sem custos adicionais, enquanto perdurar o contrato. A solução jamais poderá operar sem recursos de segurança, licenciamento ou suporte da fabricante.

1.4. PARA OS ITENS 3 E 4 DE SOFTWARE DE PROTEÇÃO

1.4.1. FUNÇÕES BÁSICAS

1.4.1.1. Todos os componentes que fazem parte da solução de segurança para desktops e servidores deverão ser fornecidos por um único fabricante, a solução de proteção a ser ofertada deverá contar com

recurso de Managed Detectionand Response da fabricante, esse recurso irá ampliar a proteção e o serviço de segurança, detecção e resposta a ameaças gerenciado 24 horas por dia, 7 dias por semana, por meio de acompanhamento direto da fabricante no ambiente interno. A prefeitura busca este recurso para melhorar a busca e investigação de ameaças, além buscar uma melhor resposta a incidentes com auxílio contratada e do fabricante;

1.4.1.2. A solução de proteção ofertada deverá dar suporte, mantendo atualizações e vacinas, para os sistemas operacionais Windows, Linux, MacOS e Windows Server, durante toda a vigência do contrato;

1.4.1.3. Em caso de descontinuidade da solução inicialmente ofertada, durante a vigência do contrato, a contratada deverá fornecer a versão mais nova ou superior ao produto ofertado, contemplando instalação e treinamento, sem custos ao município;

1.4.1.4. Deverá possuir central de monitoramento e configuração, baseada em web, totalmente em nuvem, contendo todas a ferramentas necessárias à verificação e controle da proteção dos dispositivos;

1.4.1.5. A instalação deverá ser feita via cliente específico, por download da gerência central ou também via e-mail de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas;

1.4.1.6. A solução ofertada deverá ter capacidade de realizar a análise de causas primárias e caça a ameaças conduzida por peritos da própria fabricante por meio da solução fornecida;

1.4.1.7. A console deverá permitir a segregação dos computadores, dentro da estrutura de gerenciamento em grupos;

1.4.1.8. A console deverá atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;

1.4.1.9. A console deverá permitir a aplicação de regras diferenciadas baseado em grupos ou usuários;

1.4.1.10. A console deverá permitir a definição de grupos de usuários com diferentes níveis de acesso às configurações, políticas e logs;

1.4.1.11. Deverá permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção;

1.4.1.12. Deverá possibilitar a criação e edição de diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;

1.4.1.13. Deverá fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;

1.4.1.14. Deverá permitir exclusões de escaneamento para um determinado websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política;

1.4.1.15. Deverá permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;

1.4.1.16. Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;

1.4.1.17. Atualização incremental, remota e em tempo real, da vacina de ameças e do mecanismo de verificação (Engine) dos clientes;

1.4.1.18. Deverá utilizar protocolos seguros padrão HTTPS para comunicação entre a console de gerenciamento e clientes gerenciados;

1.4.1.19. Deverá permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF;

1.4.1.20. Os Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

1.4.1.21. Deve possibilitar a exibição de informações, tais como o nome da máquina, a versão do software, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status;

1.4.1.22. Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;
1.4.1.23. Deverá fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares, procuradas palavras chaves ou informações confidenciais;
1.4.1.24. Deverá bloquear o upload ou remover a informação confidencial contida antes do envio de um arquivo que contenha esse tipo de informação;
1.4.1.25. Deverá permitir a configuração das portas de comunicação;
1.4.1.26. Deverá permitir a seleção da versão do software de preferência para um grupo de controle, permitindo assim o teste da atualização antes da implantação em toda a rede;
1.4.1.27. O agente deverá proteger laptops e desktops em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware;
1.4.1.28. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deverá fornecer controle de dispositivos USB e, controle de acesso à web;
1.4.1.29. Deverá possuir mecanismo contra a desinstalação do software pelo usuário, podendo ser definidas senhas distintas para grupos de usuários(tamper);
1.4.1.30. Deverá prover, capacidade de HIPS (Host Instrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente;
1.4.1.31. Deverá prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via web exploits;
1.4.1.32. Deverá permitir a monitoramento e o controle de dispositivos removíveis nos equipamentos dos usuários, tais como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo;
1.4.1.33. O controle de dispositivos deverá ser ao nível de permissão, somente leitura ou bloqueio;
1.4.1.34. Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis, CD, DVD, interfaces de rede sem fio, modems, bluetooth, infravermelho, além de MTP (Media TransferProtocol), tais como o Blackberry, o iPhone e o Android smartphone;
1.4.1.35. A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção projetada para a fácil administração, supervisão e elaboração de relatórios das ameaças;
1.4.1.36. Deverá possuir interface gráfica web, preferencialmente, com suporte a língua portuguesa (padrão brasileiro);
1.4.1.37. A Console de administração deverá incluir um painel com um resumo visual em tempo real para verificação do status de segurança;
1.4.1.38. Deverá exibir os dispositivos gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes da versão, etc), e classificar os computadores em conformidade;
1.4.1.39. Deverá permitir, após a identificação de um incidente, a correção dos problemas remotamente, com no mínimo as opções abaixo:
1.4.1.39.1. Proteger o dispositivo com a opção de início de uma varredura;
1.4.1.39.2. Forçar uma atualização naquele momento;
1.4.1.39.3. Ver os detalhes dos eventos ocorridos;
1.4.1.39.4. Executar verificação completa do sistema;

1.4.1.39.5. Forçar o cumprimento de uma nova política de segurança;
1.4.1.39.6. Mover o computador para outro grupo;
1.4.1.39.7. Apagar o computador da lista.
1.4.1.40. Deverá gravar um log de auditoria seguro, que monitore a atividade no console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses;
1.4.1.41. Deverá gerar relatórios, estatísticos ou gráficos, com as seguintes informações mínimas:
1.4.1.42. Usuários estão ativos, inativos ou desprotegidos, bem como seus respectivos detalhes;
1.4.1.43. Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, incluindo detalhes de alertas e das varreduras;
1.4.1.44. Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;
1.4.1.45. Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;
1.4.1.46. Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;
1.4.1.47. Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;
1.4.1.48. Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.
1.4.1.49. Deverá permitir a exportação de relatório de logs de auditoria nos formatos CSV e PDF;
1.4.1.50. Deverá conter vários relatórios para análise e controle dos usuários e computadores. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas;
1.4.1.51. Deverá fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:
1.4.1.51.1. Grupo a qual o dispositivo faz parte;
1.4.1.51.2. Status de proteção do dispositivo;
1.4.1.51.3. Último escaneamento realizado;
1.4.1.51.4. Último update;
1.4.1.51.5. Último usuário logado no dispositivo;
1.4.1.51.6. Início da proteção;
1.4.1.51.7. Nome do dispositivo.
1.4.1.52. A solução de segurança deverá possuir classificação Leader no Gartner Magic Quadrantfor Endpoint Protection Platforms, de acordo com os relatórios emitidos pelo Gartner anos de 2024.
1.4.1.53. A solução de segurança obrigatoriamente deverá ser capaz de operar de forma integrada e unificada com a solução existente na **Prefeitura Municipal de Montenegro** – RS, Switch e Acess Point Sophos.

1.4.2. DO SUPORTE TÉCNICO

1.4.2.1. A CONTRATADA deverá disponibilizar à Prefeitura de Montenegro-RS, durante toda a vigência do Contrato, uma Central de Atendimento (sítio na Internet e telefone) para aberturas e acompanhamento de chamados técnicos, das 8:00 às12:00 horas e das 13:30 às 16:30 horas, de segunda a sexta;

1.4.2.2. O atendimento será realizado de forma presencial e os chamados de assistência remota para auxilio devem ser catalogados na ferramenta de tickets/helpdesk da contratada, sendo necessário sempre o envio de e-mails com as ações realizadas;
1.4.2.3. A contratada deverá iniciar o atendimento de suporte remoto em no máximo 2 horas úteis após a abertura do chamado e solução do problema em até 4 horas;
1.4.2.4. Atendimentos que necessitem deslocamento técnico deverão ser atendidos em no máximo oito (6) horas após abertura do chamado por profissional legalmente empregado da empresa vencedora do edital;
1.4.2.5. O serviço de suporte técnico deverá ser prestado nas modalidades on-line e on-site, pela CONTRATADA, em função do nível de complexidade do chamado;
1.4.2.6. As atividades de suporte técnico incluem, mas não se restringem a prover informação, assistência e orientação para:
Instalação, desinstalação, configuração, substituição e atualização de programas (software);
1.4.2.7. Aplicação de correções (patches) e atualizações de software;
1.4.2.8. Diagnósticos, avaliações e resolução de problemas;
1.4.2.9. Ajustes finos e customização da solução obrigatoriamente serão realizados pela contratada, no, para avaliação e ameaças e riscos o trabalho deverá ser conduzido pela fabricante.
1.4.2.10. As atividades de suporte e monitoramento incluem:
1.4.2.10.1. Auxiliar o setor técnico no monitoramento de estações de trabalho com agente desativado ou software desatualizado e aplicar procedimento para sua correção;
1.4.2.10.2. Auxiliar o setor técnico a monitorar e garantir que o software esteja em 90% das estações de trabalho esteja atualizado com, no máximo, 10 (dez) dias de defasagem para a definição mais atual do fabricante da ferramenta de segurança;
1.4.2.10.3. Auxiliar o setor técnico no monitoramento dos resultados de escaneamento dos agentes por toda rede e realizar os procedimentos necessários para sanar os problemas eventualmente detectados.

1.5. DESCRIÇÃO DO ITEM 3 – LICENÇAS DE PROTEÇÃO

1.5.1. FUNÇÕES BÁSICAS

1.5.1.1. Realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos;
1.5.1.2. Buscar algum sinal de malware ativo e detectar malwares desconhecidos;
1.5.1.1. Ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para verificação de reputação, identificando possíveis arquivos maliciosos;
1.5.1.3. Realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
1.5.1.4. A solução deverá manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
1.5.1.5. Realizar a verificação de todos os arquivos no disco rígido em intervalos programados;
1.5.1.6. Realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);
1.5.1.7. Proteger os navegadores Internet Explorer (Edge), Firefox e Chrome, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

1.5.1.8. Permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
1.5.1.9. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);
1.5.1.10. Suportar máquinas com arquitetura 32 e 64 bits;
1.5.1.11. Ser compatível com os sistemas operacionais Microsoft Windows 10 e 11;
1.5.1.12. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
1.5.1.13. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção.
1.5.1.14. As soluções ofertadas devem ser contribuintes no MITRE ATT&CK de informações e técnicas de detecção. https://attack.mitre.org/resources/contribute/.

1.5.2. RECURSO DE SEGURANÇA:
1.5.2.1. Possuir atualização periódica de novas assinaturas de ataque;
1.5.2.2. Reconhecer e bloquear automaticamente as aplicações em clientes, baseando-se no hash do arquivo;
1.5.2.3. Possuir capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
1.5.2.4. Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados;
1.5.2.5. Deverá ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow;
1.5.2.6. Possuir técnicas de proteção, incluindo:
1.5.2.7. Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;
1.5.2.8. Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;
1.5.2.9. Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;
1.5.2.10. Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo.exe com a extensão .txt);
1.5.2.11. Verificação de ameaças web avançadas – bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados.

1.5.3. RECURSO DE PROTEÇÃO:
1.5.3.1. Possuir proteção em tempo real contra ameaças variadas como: worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos;
1.5.3.2. Possuir proteção anti-malware nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
1.5.3.3. As configurações do anti-spyware deverão ser realizadas através da mesma console da plataforma;

1.5.3.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;
1.5.3.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;
1.5.3.6. Possuir capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do agente de segurança;
1.5.3.7. Possuir capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;
1.5.3.8. A remoção automática dos danos causados deverá ser nativa do próprio agente; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;
1.5.3.9. Possuir capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;
1.5.3.10. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;
1.5.3.11. Proteção de Web (verificação de sites e downloads contra vírus);
1.5.3.12. Permitir o controle de acesso a sites por categoria;
1.5.3.13. Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (Firefox, Chrome e Edge), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites;
1.5.3.14. O Controle da Web deverá controlar o acesso a sites impróprios, com categorias predeterminadas de segurança e com a possibilidade de criação de listas personalizadas;
1.5.3.15. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas à console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;
1.5.3.16. Possuir capacidade de verificar somente arquivos novos e alterados;
1.5.3.17. Deverá proteger contra roubo de credenciais e contra elevação de privilégio;
1.5.3.18. Possuir funcionalidades específicas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

1.5.4. DETECÇÃO PROATIVA:

1.5.4.1. Possuir a funcionalidade de detecção de ameaças via técnicas de deep machine learning;
1.5.4.2. Possuir a funcionalidade de detecção de ameaças desconhecidas que estão em memória;
1.5.4.3. Possuir a capacidade de detecção, e bloqueio proativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);
1.5.4.4. Possuir a capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;
1.5.4.5. Possuir a capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

1.5.5. PROTEÇÃO CONTRA RAMSONWARES:

1.5.5.1. Dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;
1.5.5.2. Dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;
1.5.5.3. Prevenir ameaças e interromper que elas sejam executadas em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas;
1.5.5.4. Possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de exploração de vulnerabilidade, protegendo os dispositivos de ameaças desconhecidas e vulnerabilidades zero-day;

1.5.6. DETECÇÃO E O BLOQUEIO EXPLOIT:
1.5.6.1. Possuir funcionalidade de: DEP (Data Execution Prevention); Address Space Layout Randomization (ASLR), Load Library, Shellcode, VBScript God Mode, Application Lockdown, Process Protection Bottom Up ASLR, Full Page, Anti-HeapSpraying, Dynamics Heap Spray, Import Address Table Filtering (IAF), VTable Hijacking, Stack Pivot and Stack Exec, SEHOP, Stack-based ROP (Return-Oriented Programming), Control-Flow Integrity (CFI); Syscall; WOW64;
1.5.6.2. Network Lockdown.
1.5.6.3. A solução deverá trabalhar silenciosamente na máquina do usuário e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal realizando a limpeza e remoção completa do ransomware na máquina do usuário;
1.5.6.4. Fornecer uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados;
1.5.6.5. A console de monitoramento e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas as ferramentas para a monitoramento e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware;
1.5.6.6. A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware;

1.5.7. RECURSOS AVANÇADOS:
1.5.7.1. Possuir a capacidade de implementar técnicas de deteção e resposta, possibilitando detecção e investigação de atividades suspeitas;
1.5.7.2. Possuir a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante;
1.5.7.3. Em caso de incidente a solução deverá permitir visualizar toda a cadeia de ataque, permitindo assim análise de causa raiz;
1.5.7.4. A solução de deverá ser integrada ao agente de proteção a ser instalado com um agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
1.5.7.5. O gerenciamento da solução deverá ser feito, obrigatoriamente, a partir da mesma console de gerenciamento unificada;
1.5.7.6. Possuir resposta imediata para remediar as detecções, permitindo encerrar processos, isolar ameaças, atualizar a segurança e fazer mais varreduras;
1.5.7.7. Ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

1.5.7.8. Ser capaz de exibir todos os processos, acessos, arquivos e chaves de registros gerados pela ameaça;
1.5.7.9. Ser capaz de exibir linha de comando gerada pelo processo suspeito.
1.5.7.10. Após a análise da nuvem de inteligência do fabricante a solução deverá apresentar um relatório sobre a ameaça contendo, no mínimo:
1.5.7.11. Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;
1.5.7.12. Reputação do arquivo e correlação da detecção do arquivo em outras soluções através de bases de conhecimento ou API do Fabricante;
1.5.7.13. Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;
1.5.7.14. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, etc.;

1.5.8. CONTROLE DE APLICAÇÕES E DISPOSITIVOS:

1.5.8.1. Deverá possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;
1.5.8.2. Deverá atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas;
1.5.8.3. Deverá verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões.
1.5.8.4. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;
1.5.8.5. Deverá oferecer proteção para chaves de registro e controle de processos;
1.5.8.6. Deverá proibir, através de política a inicialização de um processo ou aplicativo, baseado em nome e no Hash do arquivo;
1.5.8.7. Deverá detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;
1.5.8.8. Deverá possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;
1.5.8.9. Deverá gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB);
1.5.8.10. Deverá permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
1.5.8.11. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;
1.5.8.12. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
1.5.8.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
1.5.8.14. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
1.5.8.15. A gestão desses dispositivos deverá ser feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos;
1.5.8.16. Deverá permitir a autorização de um dispositivo com no mínimo as seguintes opções: Todos os dispositivos do mesmo modelo; um único dispositivo, com base em seu número de identificação único; Acesso total; Acesso somente leitura; Bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

1.5.9. PROTEÇÃO E PREVENÇÃO A PERDA DE DADOS:

1.5.9.1. Deverá possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

1.5.9.2. Deverá permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

1.5.9.3. Deverá possibilitar o bloqueio, somente registrar o evento no Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

1.5.9.4. Deverá suportar a adição de regras próprias de conteúdo com um assistente fornecido para essa finalidade;

1.5.9.5. Deverá permitir a criação de regras de prevenção de perda de dados por tipo verdadeiro de arquivo;

1.5.9.6. Deverá possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

1.5.9.7. Deverá permitir o controle de dados para no mínimo os seguintes meios:

1.5.9.8. Anexado no cliente de e-mail (ao menos Outlook ou Thunderbird);

1.5.9.9. Anexado no navegador (ao menos Firefox, Chrome ou Edge);

1.5.9.10. Anexado no cliente de mensagens instantâneas (ao menos Skype);

1.5.9.11. Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

1.5.9.12. Deverá possuir listas de controle de conteúdo pré-configuradas com no mínimo as seguintes identificações:

1.5.9.13. Número de Identificação de Pessoa Física (CPF);

1.5.9.14. Número de Identificação de Pessoa Jurídica (CNPJ);

1.5.9.15. Números de cartões de crédito;

1.5.9.16. Números de Passaportes;

1.5.9.17. Endereços;

1.6. DESCRIÇÃO DO ITEM 4 – LICENÇAS DESERVIDORES

1.6.1. FUNÇÕES BÁSICAS

1.6.1.1. A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;

1.6.1.2. Deverá realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos;

1.6.1.3. O agente host deverá buscar algum sinal de malwares ativos e detectar malwares desconhecidos;

1.6.1.4. O agente deverá realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

1.6.1.5. A solução deverá manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

1.6.1.6. Deverá realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

1.6.1.7. Deverá realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

1.6.1.8. Deverá realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);
1.6.1.9. Deverá proteger os navegadores Firefox, Chrome ou Edge bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;
1.6.1.10. Deverá permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
1.6.1.11. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);
1.6.1.12. Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações;
1.6.1.13. Deverá possuir integração com a nuvem da Microsoft Azure para identificar as informações dos servidores instanciados nas nuvens;
1.6.1.14. Deverá possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
1.6.1.15. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;
1.6.1.16. Deverá possuir funcionalidade de controlar aplicações, permitindo criar uma lista de aplicações que poderão ser executadas no servidor. Todas as aplicações não listadas deverão ser bloqueadas sua execução.
1.6.1.17. O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais abaixo:
1.6.1.17.1. Windows Server 2019, 2022 e 2025;
1.6.1.17.2. Debian 11 e 12;
1.6.1.17.3. CentOS Stream;
1.6.1.17.4. Ubuntu 20.04, 22.04 e 24.04;
1.6.1.17.5. SUSE Enterprise 15;

1.7.1. FUNCIONALIDADE DE PROTEÇÃO AVANÇADA:
1.7.1.1. Deverá possuir proteção contra exploração de buffer overflow;
1.7.1.2. Deverá possuir proteção contra-ataques de Negação de Serviço (Denialof Service - DoS), PortScan, MAC Spoofing e IP Spoofing;
1.7.1.3. Deverá possuir atualização periódica de novas assinaturas de ataque;
1.7.1.4. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo;
1.7.1.5. Deverá possuir capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
1.7.1.6. Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados;
1.7.1.7. Deverá ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow;
1.7.1.8. Deverá possuir técnicas de proteção, que inclui:
1.7.1.8.1. Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;
1.7.1.8.2. Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;

1.7.1.8.3. Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;
1.7.1.8.4. Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);
1.7.1.8.5. Verificação de ameaças web avançadas - bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

1.7.2. DETECÇÃO DE AMEÇAS:

1.7.2.1. Deverá realizar proteção em tempo real contra ameaças, tipo: trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos;
1.7.2.2. Deverá realizar proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
1.7.2.3. As configurações do anti-spyware deverão ser realizadas através da mesma console da solução;
1.7.2.4. Deverá permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;
1.7.2.5. Deverá permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;
1.7.2.6. Deverá possuir capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do agente;
1.7.2.7. Deverá possuir capacidade de detectar arquivos através da reputação dos mesmos;
1.7.2.8. Deverá possuir capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;
1.7.2.9. A remoção automática dos danos causados deverá ser nativa do próprio agente; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;
1.7.2.10. Deverá possuir capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;
1.7.2.11. Deverá detectar tráfego de rede para comandar e controlar os servidores;
1.7.2.12. Deverá proteger arquivos de documento contra-ataque do tipo ransomwares;
1.7.2.13. Deverá proteger que o ataque de ransomware seja executado remotamente;
1.7.2.14. Deverá permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante;
1.7.2.15. Deverá permitir o bloqueio da verificação de vírus em recursos mapeados da rede;
1.7.2.16. Proteção Web (verificação de sites e downloads contra vírus);
1.7.2.17. Deverá realizar controle de acesso a sites por categoria de segurança;
1.7.2.18. Deverá proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (Firefox, Chrome e Edge), fornecendo controle da Internet independentemente do browser utilizado sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites;
1.7.2.19. O Controle da Web deverá controlar o acesso a sites impróprios, com categorias predeterminadas de segurança e com a possibilidade de criação de listas personalizadas;

1.7.2.20. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;
1.7.2.21. Deverá possuir capacidade de verificar somente arquivos novos e alterados;
1.7.2.22. Deverá proteger contra roubo de credenciais e contra elevação de privilégio;
1.7.2.23. Deverá possuir funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração;
1.7.2.24. Deverá possuir capacidade de habilitar mensagens de desktop para a proteção contra ameaças;
1.7.2.25. Deverá possuir capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas;

1.7.3. RECONHECIMENTO DE NOVAS AMEAÇAS:
1.7.3.1. Deverá possuir funcionalidade de detecção de ameaças via técnicas de deep machine learning;
1.7.3.2. Deverá possuir funcionalidade de detecção de ameaças desconhecidas que estão em memória;
1.7.3.3. Deverá possuir capacidade de detecção, e bloqueio proativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);
1.7.3.4. Deverá possuir capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;
1.7.3.5. Deverá possuir capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

1.7.4. PROTEÇÃO CONTRA RANSOMWARES:
1.7.4.1. Deverá dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;
1.7.4.2. Deverá dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;
1.7.4.3. Deve dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

1.7.5. DETECÇÃO AVANÇADA:
1.7.5.1. A solução deverá ter capacidade de implementar técnicas de detecção e resposta, possibilitando detecção e investigação nos servidores com atividades suspeitas;
1.7.5.2. Deverá ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.
1.7.5.3. Em caso de incidente a solução deverá mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.
1.7.5.4. Após a análise da nuvem de inteligência do fabricante, a solução deverá apresentar um relatório sobre a ameaça contendo no mínimo:
1.7.5.5. Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;
1.7.5.6. Reputação do arquivo e correlação da detecção do arquivo em outras soluções através de bases de conhecimento ou API do Fabricante;
1.7.5.7. Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;
1.7.5.8. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, etc.;
1.7.5.9. A solução de detecção e resposta deverá ser integrada ao agente a ser instalado com um agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

1.7.5.10. O gerenciamento da solução de detecção e resposta deverá, preferencialmente, ser feito a partir da mesma console de gerenciamento da solução;
1.7.5.11. Deverá fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;
1.7.5.12. Deverá ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;
1.7.5.13. Deverá ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;
1.7.5.14. Deverá ser capaz de exibir todos os processos, acessos, arquivos e chaves de registros gerados pela ameaça;
1.7.5.15. Deverá ser capaz de exibir linha de comando gerada pelo processo suspeito.

1.7.6. CONTROLE DE APLICAÇÕES:

1.7.6.1. Deverá possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;
1.7.6.2. Deverá atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicações possam ser liberadas ou bloqueadas;
1.7.6.3. Deverá verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;
1.7.6.4. Deverá oferecer proteção para chaves de registro e controle de processos;
1.7.6.5. Deverá proibir através de política a inicialização de um processo ou aplicativo baseado em nome e no Hash do arquivo;
1.7.6.6. Deverá detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;
1.7.6.7. Deverá possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;
1.7.6.8. As funcionalidades relacionadas ao controle de aplicações deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins, sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
1.7.6.9. Deverá possuir capacidade de bloquear execução de aplicativo que está em armazenamento externo;

1.8. DESCRIÇÃO DO ITEM 5 – SOFTWARE DE GESTÃO

1.8.1. SOFTWARE DE GERENCIAMENTO E INVENTÁRIO

1.8.1.1 Realizar inventário de Hardware. A solução deve inventariar os ativos de Hardware, coletando informações sobre computadores e seus componentes, impressoras e demais equipamentos. Exemplo de informações que devem constar no inventário: fabricante, nome do modelo, número de série, processador, placa-mãe, disco rígido, placa de vídeo, de rede, memória RAM, etc;
1.8.1.2 A solução deve possuir inventário de Softwares instalados em dispositivos Windows e Linux da rede, possibilitando seu registro e controle de licenciamento;
1.8.1.3 A solução deve realizar a medição do uso do software, informando a quantidade e duração de uso de um determinado software por um usuário e/ou estação de trabalho;
1.8.1.4 A solução deve permitir o registro das licenças existentes para cada software, a data de expiração das mesmas e o controle de quantas licenças estão sendo utilizadas e quantas estão ociosas. Deve

identificar quais são os computadores que estão utilizando cada licença, gerar avisos quando há mais licenças do software em uso do que o número de licenças disponíveis;
1.8.1.5 A solução deve permitir a instalação de um agente único para obter todas informações e dados necessários, além disso o agente deverá permitir acesso remoto diretamente nos computadores instalados, sem necessidade de instalação de outros softwares;
1.8.1.6 A solução deve permitir o controle de registro, processos e arquivos, sem a necessidade de acesso remoto diretamente do computador em manutenção;
1.8.1.7 Deve ser possível, através da solução, distribuir e reinstalar softwares e aplicativos para um ativo específico, assim como para um grupo ou para a totalidade de equipamentos da rede corporativa.
1.8.1.8 Deve ser possível agendar (dia/semana/mês) a instalação ou mesmo fazê-la em tempo real;
1.8.1.9 A solução deve implementar a funcionalidade de realizar a desinstalação de softwares e aplicativos em um equipamento específico, assim como para um grupo ou para a totalidade de equipamentos da rede corporativa. Deve ser possível agendar a desinstalação ou mesmo fazê-la em tempo real;
1.8.1.10 A solução deve permitir, através de sua interface administrativa, que os técnicos acessem remotamente computadores em manutenção para realizar tarefas como: iniciar ou parar um serviço, alterar o registro, apagar ou criar um arquivo e/ou pasta, renomear um computador ou parar um processo em execução;
1.8.1.11 A solução deve ter seu console de gestão instalado e configurado na nuvem, sem necessidade de máquina virtual, servidor ou licença.
adicional de sistema operacional ou banco de dados para plena operação da plataforma;
1.8.1.12 A solução deve identificar ativos de diferentes Sistemas Operacionais (Windows e Linux), isso visa ampliar a portabilidade da solução, permitindo reconhecer e coletar informações de dispositivos Windows e Linux;
1.8.1.13 A solução deve possuir Interface Web ou padrão Windows, o que permite que o acesso às suas funcionalidades seja realizado via interface web ou padrão Windows, com autenticação de duplo fator;
1.8.1.14 A solução deve realizar o gerenciamento de Bitlocker e com isso deve permitir ativar e desativar o Bitlocker em estações de trabalho, assim como armazenar a chave de recuperação de cada disco criptografado;
1.8.1.15 A solução deverá permitir a Implantação de Sistema Operacional, através de módulo adicional que possa permitir a implantação de imagens de sistema operacional remotamente;
1.8.1.16 A solução deverá possibilitar autogerenciamento de aplicativos pelos usuários. A solução deve possibilitar que o usuário instale/desinstale aplicativos pré-definidos através de um portal de autoatendimento;
1.8.1.17 A solução deverá realizar o gerenciamento de Patches, do Sistema Operacional e de aplicativos de terceiros. Ainda, a solução deve permitir a automatização na implantação de patches de segurança e de melhoria;
1.8.1.18 A solução deverá realizar suporte à tecnologia, com gerenciamento do setup dos computadores e atividades correlatas, como ligar, desligar, reiniciar os computadores remotamente, via console, sem necessidade de acesso direto com usuário administrador em cada computador;
1.8.1.19 A solução deverá permitir a inclusão de campos adicionais no cadastro de ativos para hardware e software O campo deve permitir incluir as informações: Nº do contrato, objeto do contrato, fiscais do contrato, tipo, marca/modelo, valor, fornecedor, responsáveis pelos equipamentos (demandante, técnico e administrativo), garantia dos equipamentos, status (ativo/inativo), classificação de criticidade e identificador;

1.8.1.20 A solução deverá realizar e permitir o registro de informações dos bancos de dados corporativos, bem como o controle de licença dos bancos de dados utilizados nos servidores corporativos;
1.8.1.21 A solução deverá possuir Banco de Dados Centralizado para armazenamento automático das informações referentes aos ativos e itens de configuração, estar de acordo com o definido no ITIL v3. Deverá fazer integração entre os ativos, seus atributos e a relação entre eles, de forma automática;
1.8.1.22 A solução deverá realizar a gestão de Ativos e Patches. Deverão estar integradas entre si, através de uma base de dados, fazendo parte de uma mesma solução, podendo ser ofertadas por módulos;
1.8.1.23 A solução deverá realizar consultas, relatórios e dashboards. As consultas e relatórios acessíveis pela console Web ou padrão Windows, com pesquisas parametrizáveis, permitindo exibição por gráficos e exportação para vários formatos de arquivos do mercado, como por exemplo, .csv e .pdf;
1.8.1.24 A solução deverá ser robusta e bem avaliada e para tanto será aceita solução contemplada no 2023 Gartner Market Guide for UEM tools ou classificada como Strong no UnifiedEndpoint Management do Forrester;
1.8.1.25 A solução deve realizar o gerenciamento de patches de Sistema Operacional e de aplicativos de terceiros, de forma automática. Ainda, a solução deve permitir a automatização na implantação de patches de segurança e de melhoria. Gerenciamento de patch deve controlar multi-dependências de patches, ou seja, se há múltiplos pacotes sendo instalados, requerendo múltiplos reboots, o agente suprime os reboots até que tudo esteja completo. Deve apontar todas as versões da aplicação que são afetadas e precisam de correção;
1.8.1.26 A solução deve possuir centralizado o armazenamento automático das informações referentes aos ativos e itens de configuração e estar de acordo com o definido no ITIL v3. Possuir banco de dados de patches de correção que seja atualizado de forma contínua, a partir do site dos fabricantes. O catálogo de patches a serem aplicados deve filtrar de forma simples quais são os patches que precisam ser instalados e exibir somente as últimas versões disponíveis de cada um deles, considerando a obsolescência de versões antigas;
1.8.1.27 A solução deve permitir consultas, relatórios e dashboards pela console Web ou padrão Windows, com pesquisas parametrizáveis, permitindo exibição por gráficos e exportação para vários formatos de arquivos do mercado, como por exemplo, .csv e .pdf. O status individual de cada tarefa de patch deve mostrar quais patches foram instalados com sucesso, que falharam e quais não foram instalados por não serem necessários;
1.8.1.28 A solução deve permitir uso de políticas impositivas de aplicações nos computadores, a plataforma forma de gerenciamento deverá estar operacional via web cloud, não sendo necessários servidores locais para gerenciamento, apenas a instalação do agent;
1.8.1.29 A solução deve realizar a distribuição dos patches e agentes, com isso prover a instalação remota, automática e silenciosa do agente, quando houver. Deve permitir o download de patches antes do início da tarefa, de forma a otimizar o processo de instalação;
1.8.1.30 A solução deve permitir que o acesso às suas funcionalidades seja realizado via interface web ou padrão Windows, com autenticação de duplo fator;
1.8.1.31 A solução deve ter a Administração baseada em regras, permitindo segmentar níveis de acesso por perfis de usuários, como por exemplo, administradores, operadores;
1.8.1.32 A solução deve prover integração com o LDAP ou Microsoft Active Directory, permitindo a fácil instalação dos agentes de report em cada computador;
1.8.1.33 A solução deve possuir função escanear por máquina para busca de informações sobre os patches não instalados e confrontá-los contra o banco de dados de patches disponíveis;

1.8.1.34 A solução deve possuir recurso para configuração da periodicidade de sincronização do banco de dados de patches, possuir recurso para testar e aprovar os patches antes do processo de deploy;
1.8.1.35 A solução deve conter a inteligência de filtrar automaticamente, sem intervenção, quais ativos receberão os patches selecionados na tarefa de patch considerando a arquitetura do sistema operacional e também a pré-existência de determinada aplicação, evitando assim instalações indesejadas;
1.8.1.36 A solução deve todos terminais da rede interna, dessa forma deverá ser considerado o conjunto de licença que possa cobrir no mínimo 820 computadores/terminais.

1.8.2. DO SUPORTE TÉCNICO

1.8.2.1. A CONTRATADA deverá disponibilizar à Prefeitura de Montenegro-RS, durante toda a vigência do Contrato, uma Central de Atendimento via web para aberturas e acompanhamento de chamados técnicos, 24x7, e via telefone, das 8:00 às12:00 horas e das 13:30 às 16:30 horas, de segunda a sexta;
1.8.2.2. O atendimento será realizado de forma presencial e os chamados de assistência remota para auxilio devem ser catalogados na ferramenta de tickets/helpdesk da contratada, sendo necessário sempre o envio de e-mails com as ações realizadas;
1.8.2.3. A contratada deverá iniciar o atendimento de suporte remoto em no máximo 2 horas úteis após a abertura do chamado e solução do problema em até 4 horas;
1.8.2.4. Atendimentos que necessitem deslocamento técnico deverão ser atendidos em no máximo oito (8) horas após abertura do chamado por profissional legalmente empregado da empresa contratada;
1.8.2.5. O serviço de suporte técnico deverá ser prestado nas modalidades on-line e on-site, pela CONTRATADA, em função do nível de complexidade do chamado;
1.8.2.6. As atividades de suporte técnico incluem, mas não se restringem a prover informação, assistência e orientação para:

a) Instalação, desinstalação, configuração, substituição e atualização de programas (software);
b) Aplicação de correções (patches) e atualizações de software;
c) Diagnósticos, avaliações e resolução de problemas;
d) Ajustes finos e customização da solução obrigatoriamente serão realizados pela contratada, no, para avaliação e ameaças e riscos o trabalho deverá ser conduzido pela fabricante.
e) As atividades de suporte e monitoramento incluem:
f) Auxiliar o setor técnico no monitoramento de estações de trabalho com agente desativado ou software desatualizado e aplicar procedimento para sua correção;
g) Auxiliar o setor técnico a monitorar e garantir que o software de proteção esteja em 90% das estações de trabalho esteja atualizado com, no máximo, 10 (dez) dias de defasagem para a definição mais atual do fabricante da ferramenta de segurança;
h) Auxiliar o setor técnico no monitoramento dos resultados de escaneamento dos agentes por toda rede e realizar os procedimentos necessários para sanar os problemas eventualmente detectados.

1.9. DESCRIÇÃO DO ITEM 6 – PLATAFORMA DE PROTEÇÃO E CDN

1.9.1. PLATAFORMA DE PROTEÇÃO E CDN

1.9.1.1. A solução deve possuir proteção DDoSintegrada.

1.9.1.2. A solução deve possuir recurso de CDN.
1.9.1.3. A solução deve possuir capacidade de uso de certificado SSL universal.
1.9.1.4. A solução deve possuir recurso de segurança tipo WAF nativo em cloud.
1.9.1.5. A solução deve possuir acelerador de imagens.
1.9.1.6. A solução deve possuir recurso de AMP, acelerador de aplicativos moveis.
1.9.1.7. A solução deve possuir e/ou realizar a gestão e controle de acesso e logins baseados em função.
1.9.1.8. A solução deve possuir mecanismo de detecção de ameaças capaz de operar em até 150 regras WAF.
1.9.1.9. A solução deve possuir mecanismo avançado de deteção de BOTs.
1.9.1.10. A solução deve possuir capacidade para gestão de até 100 hotnames.
1.9.1.11. A solução deve possuir capacidade para gerenciamento total de DNS, com suporte a MX, TXT, @ entre outros.
1.9.1.12. A solução deve possuir capacidade de atuar com DNSSec diretamente com o Registro BR.
1.9.1.13. A solução deve possuir monitor de integridade de balanceamento de carga.
1.9.1.14. A solução deve possuir capacidade de realizar armazenamento em camadas.
1.9.1.15. A solução deve possuir capacidade de até 20 regras por páginas.
1.9.1.16. A solução deve possuir de gerenciamento de conexões IPv6 e HTTP/2.
1.9.1.17. A solução deve possuir de otimização de imagens Polish.
1.9.1.18. A solução deve possuir capacidade de realizar até 5.000 transformações de imagens.
1.9.1.19. A solução deve possuir recurso para detenção novas ameaças.
1.9.1.20. A solução deve possuir recurso de proteção de ameaças com base na reputação da origem.
1.9.1.21. A solução deve possuir WAF com recurso e controle de GEPIP, controle de bot.
1.9.1.22. A solução deve possuir alerta de ataque DDoS
1.9.1.23. A solução deve possuir modo de ataque para aumentar a segurança da página WEB de forma Wizards.
1.9.1.24. A solução deve possuir recurso de implementação de desafio Captcha/JS.
1.9.1.25. A solução deve possuir mecanismo de combate efetivo de Bots.
1.9.1.26. A solução deve possuir recurso e controle de regras OWASP.
1.9.1.27. A solução deve possuir capacidade de realizar varredura de credenciais expostas.
1.9.1.28. A solução deve possuir capacidade de implementar rate limite sobre IP de origem.
1.9.1.29. A solução deve permitir registro coringas de DNS.
1.9.1.30. A solução deve proteger acesso a servidores internos por meio de recursos de Proxy, no qual os acesos primeiro é realizado a rede ao CDN para depois ser efetivamente enviado a rede/link.
1.9.1.30. Para acesso a solução a proponente deverá prover os recursos de acessos seguro, conforme indicado a seguir, para até 5 acessos:
1.9.1.30.1. Chave de segurança(hardkey) compatível com a solução de segurança ofertada.
1.9.1.30.2. Deverá ser compatível com FIDO2, FIDO U2F, OATH, SmartCard, OpenPGP e OTP.
1.9.1.30.3. Deverá ter certificação FIDO U2F, FICO2 e FIDO Level 2.
1.9.1.30.4. Possuir conexões tipo USB-A e NFC para comunicação com dispositivos.
1.9.1.30.5. Possuir as seguintes criptografias: RSA 2048, ECC p256 e ECDSA.
1.9.1.30.6. Grau de proteção IP68;
1.9.1.30.7. Suporte a 2FA.
1.9.1.30.8. Deverá ser compatível com a solução proposta e compatível com Microsoft e Google.
1.9.1.30.9. Deverá ser fornecida 5 chaves de acesso durante a vigência contratual.
1.9.1.31. A solução deve realizar o controle e a gestão de 1 domino de DNS montenegro.rs.gov.br com todas funcionalidades ativadas indicadas no termo de referência.

1.9.1.32. A solução deve possuir capacidade de realizar proxy de acesso DNS.
1.9.1.33. A solução deve possuir capacidade de acesso via API de integração.
1.9.1.34. A solução deve possuir recurso de Analyts.
1.9.1.35. A solução deve possuir capacidade de exportar eventos em CSV.
1.9.1.36. A solução deve ser compatível com as normas ISO 27001.
1.9.1.37. A solução deve possuir capacidade efetiva de proteção a serviços de DNS, com hospedagem completa de registro.
1.9.1.38. A solução deve possuir wizard de migração com cópia dos registros atuais do domínio.

1.10. DESCRIÇÃO DO ITEM 7 – INSTALAÇÃO DOS ITENS

1.10.1. DOS ITENS 1 E 2

1.10.1.1. Os pagamentos mensais referentes à locação de serviço de solução integrada" Appliance" de que trata os ITENS 1 e 2, iniciar-se-ão somente após a conclusão dos serviços de instalação;
1.10.1.2. O prazo para instalação é de até 10 (Dez dias) dias contados a partir da assinatura do contrato;
1.10.1.3. Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, customização, funcionalidades e políticas, bem como posteriores possíveis mudanças de local;
1.10.1.4. A contratada deverá realizar conectorização e energização do equipamento e demais conexões do equipamento na rede lógica para permitir gerência do equipamento através da rede da Prefeitura Municipal de Montenegro;
1.10.1.5. A contratada deverá realizar a migração das regras e filtragem de conteúdo existente para a nova solução proposta, permitindo assim o mínimo de impacto no ambiente;
1.10.1.6. A migração deve ser efetuada em janelas de horários a combinar com de informática, de forma que não prejudiquem a prestação de serviços ao cidadão;
1.10.1.7. A contratada deverá realizar a habilitação e configuração de todas as funcionalidades citadas neste termo de referência, desde que tenham utilidade no ambiente computacional desta prefeitura;
1.10.1.8. A instalação deve ser feita por técnicos treinados e certificados;
1.10.1.9. A contratada deverá realizar acompanhamento técnico presencial mínimo de 40 horas no ambiente posterior à instalação para avaliar se as regras e o tráfego de rede do equipamento não estão afetando a atividade fim desta prefeitura.
1.10.1.10. A contratada deverá cumprir os prazos estipulados nos cronogramas acordados e aprovados com esta Prefeitura;
1.10.1.11. A contratada deverá realizar a instalação dos equipamentos em rack 19";
1.10.1.12. A contratada deverá realizar ativação do sistema operacional, com instalação da licença e demais particularidades do equipamento;
1.10.1.13. A contratada deverá realizar a ativação contemplando a criação de usuários para administração e gerência do equipamento.
1.10.1.14. A contratada deverá realizar a integração com Microsoft Active Directory para que possa realizar a autenticação dos usuários automaticamente com as credenciais de acesso ao computador;
Toda a despesa de deslocamento e hospedagem, deve ser de responsabilidade da contratada;
1.10.1.15. A contratada deverá realizar a integração de todos os softwares e componentes de segurança necessário para o pleno atendimento do termo de referência, deverá ser utilizado todos manuais guias da fabricante de boas práticas para o pleno atendimento do serviço de segurança.

1.10.2. DOS ITENS 3 E 4

1.10.2.1. O prazo é de até 10 dias para INÍCIO da instalação, contados a partir da assinatura do contrato, e de até 20 (vinte) dias para CONCLUSÃO, contados a partir da assinatura do contrato;
1.10.2.2. A contratada deverá realizar o serviço de instalação e customização das regras gerais dos softwares com base em cada tipo de solução, deverá ser realizado de forma presencial na secretaria de administração, sendo acompanhado pelos técnicos desta Prefeitura;
1.10.2.3. A contratada deverá realizar a configuração da plataforma como forma de facilitar a instalação, automatizando o processo nos computadores conectados ao domínio na rede da contratante, podendo ser realizado de forma remota;
1.10.2.4. A contratada deverá instruir equipe técnica da contratante para realização do serviço de instalação deste agente de segurança em todas as máquinas que estiverem fora do domínio;
1.10.2.5. Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da contratada.

1.10.3. DOS ITENS 5 E 6

1.10.3.1. O prazo é de até 10 dias para INÍCIO da instalação, contados a partir da assinatura do contrato, e de até 20 (vinte) dias para CONCLUSÃO, contados a partir da assinatura do contrato;
1.10.3.2. A contratada deverá realizar o serviço de instalação e customização das regras gerais dos softwares com base em cada tipo de solução, deverá ser realizado de forma presencial na secretaria de administração, sendo acompanhado pelos técnicos desta Prefeitura;
1.10.3.3. A contratada deverá realizar a configuração da plataforma como forma de facilitar a instalação, automatizando o processo nos computadores conectados ao domínio na rede da contratante, podendo ser realizado de forma remota;
1.10.3.4. A contratada deverá instruir equipe técnica da contratante para realização do serviço de instalação todas as máquinas que estiverem fora do domínio;
1.10.3.5. Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da contratada.
1.10.3.6. A migração dos serviços de DNS e demais componentes agregados devem ser realizados de forma a não impactar o ambiente computacional.
1.10.3.7. A implantação do novo software de gerenciamento e acesso remoto, poderá exigir a remoção da ou das ferramentas pré-existentes no ambiente, caberá a contratada efetuar todo o serviço de remoção e implantação da nova ferramenta.
1.10.3.8. A implantação do novo software de gerenciamento e acesso remoto, será necessário a customização para implantação automatizada via AD ou através de forma de implantação do software.

1.11. DESCRIÇÃO DO ITEM 6 – TREINAMENTO DAS SOLUÇÕES CONTRATADAS

1.11.1. DO TREINAMENTO DO APPLIANCE

1.11.1.1. O prazo para início da execução do treinamento é de até 60 (SESSENTA) dias contados a partir da assinatura do contrato;
1.11.1.2. Deverá ser fornecido treinamento da solução da adquirida (hardware e software) para uma equipe de 04 (quatro) pessoas designadas pela contratante por um período mínimo de 12 horas;
1.11.1.3. O instrutor deverá ser certificado pelo fabricante da solução de segurança no nível técnico mais elevado dentro da fabricante, esta comprovação será realizada obrigatoriamente mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação, no momento da habilitação da licitante;
1.11.1.4. A contratada deverá fornecer todo material para o treinamento;

1.11.1.5. Toda a infraestrutura, os custos de material (apostilas, manuais, etc.), alimentação do instrutor e instrutor (deslocamento, hospedagem e vencimentos) ficará a cargo da CONTRATADA;
1.11.1.6. O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;
1.11.1.7. Deve ser incluído, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada;
1.11.1.8. Este treinamento deverá ser realizado de forma presencial, dentro do município da CONTRATANTE e em local a ser definido pela secretaria de administração;
1.11.1.9. Os cursos deverão ser realizados em horários e datas a serem acordados pela CONTRATADA e CONTRATANTE.

1.11.2. DO TREINAMENTO DO SOFTWARE DE PROTEÇÂO

1.11.2.1. O prazo para a execução do treinamento é de até 10 (dez) dias contados a partir do treinamento da ferramenta anterior;
1.11.2.2. Deverá ser fornecido treinamento implantada para uma equipe de até 05 (cinco) pessoas designadas pela contratante por um período mínimo de 6 horas;
1.11.2.3. A contratada deverá fornecer todo material para o treinamento;
1.11.2.4. Os custos de material (apostilas, manuais, etc.), alimentação do instrutor e instrutor (deslocamento, hospedagem e vencimentos) ficará a cargo da CONTRATADA;
1.11.2.5. O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;
1.11.2.6. Deve ser incluído, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada;
1.11.2.7. O instrutor deverá ser certificado pelo fabricante da solução de segurança no nível técnico mais elevado, esta comprovação obrigatoriamente será realizada mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação, no momento da habilitação da licitante;
1.11.2.8. Este treinamento deverá ser realizado de forma presencial, dentro do município da CONTRATANTE e em local a ser definido pela secretaria de administração;
1.11.2.9. Os cursos deverão ser realizados em horários e datas a serem acordados pela CONTRATADA e CONTRATANTE.

1.11.3. DO TREINAMENTO DO SOFTWARE GERENCIAMENTO

1.11.3.1. O prazo para a execução do treinamento é de até 10 (dez) dias contados a partir do treinamento da ferramenta anterior;
1.11.3.2. Deverá ser fornecido treinamento implantada para uma equipe de até 05 (cinco) pessoas designadas pela contratante por um período mínimo de 6 horas;
1.11.3.3. A contratada deverá fornecer todo material para o treinamento;
1.11.3.4. Os custos de material (apostilas, manuais, etc.), alimentação do instrutor e instrutor (deslocamento, hospedagem e vencimentos) ficará a cargo da CONTRATADA;
1.11.3.5. O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;
1.11.3.6. Deve ser incluído, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada;
1.11.3.7. Este treinamento deverá ser realizado de forma presencial, dentro do município da CONTRATANTE e em local a ser definido pela secretaria de administração;

1.11.3.8. Os cursos deverão ser realizados em horários e datas a serem acordados pela CONTRATADA e CONTRATANTE.

1.11.4. DO TREINAMENTO DA PLATAFORMA CDN

1.11.4.1. O prazo para a execução do treinamento é de até 10 (dez) dias contados a partir do treinamento da ferramenta anterior;

1.11.4.2. Deverá ser fornecido treinamento implantada para uma equipe de até 05 (cinco) pessoas designadas pela contratante por um período mínimo de 6 horas;

1.11.4.3. A contratada deverá fornecer todo material para o treinamento;

1.11.4.4. Os custos de material (apostilas, manuais, etc.), alimentação do instrutor e instrutor (deslocamento, hospedagem e vencimentos) ficará a cargo da CONTRATADA;

1.11.4.5. O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;

1.11.4.6. Deve ser incluído, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada;

1.11.4.7. Este treinamento deverá ser realizado de forma presencial, dentro do município da CONTRATANTE e em local a ser definido pela secretaria de administração;

1.11.4.8. Os cursos deverão ser realizados em horários e datas a serem acordados pela CONTRATADA e CONTRATANTE.

2. VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 60 meses contados da data de assinatura do contrato, prorrogável por igual período, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.2. O fornecimento de bens (hardwares, softwares e licenças) é enquadrado como continuado tendo em vista que há a necessidade do constante acompanhamento, ajuste e atualização do serviço e manutenção preventiva e ativa da solução sendo a vigência plurianual mais vantajosa considerando o Estudo Técnico Preliminar.

3. CLASSIFICAÇÃO DOS SERVIÇOS E FORMA DE PRESTAÇÃO

3.1. O objeto a ser contratado enquadra-se na classificação de serviços contínuos, nos termos do inciso XV, art. 6º da Lei n.º 14.133/2021.

3.2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme § 2º do art. 24 do Decreto Municipal nº 9.555, de 11 de janeiro de 2024.

3.3. Forma de fornecimento:

3.3.1. O fornecimento do objeto será continuado.

CAPÍTULO II
DA FUNDAMENTAÇÃO DA CONTRATAÇÃO, DESCRIÇÃO DA SOLUÇÃO E REQUISITOS DA

PREFEITURA MUNICIPAL DE MONTENEGRO

CONTRATAÇÃO

4. NECESSIDADE DA CONTRATAÇÃO

4.1. A necessidade da contratação como um todo encontra-se pormenorizada no item 1 do Estudo Técnico Preliminar.

5. DESCRIÇÃO DASOLUÇÂO

5.1 A descrição da solução como um todo encontra-se pormenorizada no item 1.1 deste Termo de Referência.

6. REQUISITOS DA CONTRATAÇÃO

PARTICIPAÇÃO DE EMPRESAS REUNIDAS EM CONSÓRCIO:

6.1. Será permitida a participação de empresas reunidas em consórcio:

() Não. Justificar:
(X) Sim.

6.1.1. O licitante vencedor é obrigado a promover, antes da celebração do contrato, a constituição e o registro do consórcio, nos termos do art. 15, § 3º da Lei n.º 14.133/2021.

SUBCONTRATAÇÃO

6.2. Não é admitida a subcontratação do objeto deste Termo de Referência.

GARANTIA DA CONTRATAÇÃO

6.3. Não haverá exigência da garantia da contratação dos art. 96 e seguintes da Lei nº 14.133, de 2021.

GARANTIA, MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

6.4. O prazo de garantia é aquele estabelecido na Lei n.º 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

6.5. A descrição da Manutenção e Assistência Técnica está pormenorizada no Item 5 deste Termo de Referência uma vez que fazem parte da Solução à ser contratada.

DA EXIGÊNCIA DE AMOSTRA

6.6. Haverá necessidade de apresentação de prova de conceito:

(X) Não.
( ) Sim. Justificar:

LEGISLAÇÃO TÉCNICA APLICÁVEL

6.7. Existe legislação técnica aplicável ao objeto contratado.

(X) Não ( ) Sim

INDICAÇÃO/VEDAÇÃO DE MARCA, MODELOS OU PRODUTOS (Art. 41, inciso I, da Lei nº 14.133, de 2021)

Indicação de Marcas ou Modelos

6.8. Na presente contratação será admitida a indicação da(s) seguinte(s) marca(s), característica(s) ou modelo(s), de acordo com as justificativas contidas nos Estudos Técnicos Preliminares: SOPHOS.

Da Vedação de Contratação de Marca ou Produto

6.9. Diante da justificativa contida no Estudo Técnico Preliminar, não poderão ser aceitas soluções que não permitem a integração nativa com equipamentos Sophos (switches e acess points).

CAPÍTULO III
DO MODELO DE EXECUÇÃO DO OBJETO

7. DESCRIÇÃO DA FORMA DEPRESTAÇÃO DOS SERVIÇOS

CONDIÇÕES DE EXECUÇÃO

7.1. A execução do objeto seguirá a seguinte dinâmica:

7.1.1. A execução dos serviços será realizada de forma presencial e remota, conforme a etapa do projeto e a natureza da atividade. Inicialmente, a contratada será responsável pela entrega, instalação física e configuração completa dos equipamentos de segurança de rede (firewalls), com integração à infraestrutura existente da Prefeitura, incluindo switches, access points, servidores, controladores e diretórios ativos (AD).

A contratada deverá empregar metodologias reconhecidas e melhores práticas do mercado para aplicação das políticas de segurança, segmentação de rede, controle de tráfego, regras de acesso e demais ajustes técnicos necessários. A solução deverá ser integrada a uma plataforma de gerenciamento em nuvem, garantindo controle centralizado, visibilidade contínua e facilidade de administração.

7.1.2. O cronograma de execução será elaborado em conjunto com a contratante durante a fase inicial do contrato, e deverá contemplar:

- Entrega e instalação dos equipamentos;
- Configuração e integração completa com os ativos de rede;
- Testes de operação, inspeção de tráfego e validação de regras;
- Integração com a plataforma em nuvem e painel de gerenciamento;
- Capacitação da equipe técnica da contratante;
- Elaboração de relatórios técnicos e documentação de aceite.

7.1.3. Após a implantação, o ambiente deverá operar de forma autônoma e estável, com atuação da contratada sempre que houver necessidade de suporte, atualização, reconfiguração, análise de incidentes ou implementação de melhorias. A contratada deverá manter a documentação atualizada e atuar em estreita colaboração com a equipe técnica da contratante.

ROTINAS A SEREM CUMPRIDAS

7.2. A execução contratual observará as seguintes rotinas:

7.2.1. A contratada deverá manter canais de atendimento disponíveis (portal, e-mail e telefone) para registro de chamados técnicos, abrangendo falhas, alterações de configuração, criação de novas regras, atualização de firmware e demais solicitações. O atendimento deverá observar os prazos definidos neste Termo de Referência.

7.2.2. Durante a vigência contratual, a contratada será responsável por:

- Realizar intervenções presenciais ou remotas, quando necessário, para garantir o funcionamento pleno e seguro da solução;
- Aplicar correções e atualizações de segurança conforme orientações do fabricante ou solicitações da contratante;
- Apoiar tecnicamente a contratante na implementação de novas regras, ajustes de segmentação de rede e políticas de acesso;
- Analisar periodicamente o ambiente, sugerindo melhorias, otimizando a performance e propondo medidas de mitigação de riscos;
- Participar de reuniões técnicas, quando convocada, para alinhamento estratégico, análise de ameaças e definição de ações preventivas;
- Emitir relatórios técnicos de suporte e intervenções, conforme aplicável.

8. DO PRAZO, LOCAL E HORÁRIO DE PRESTAÇÃO DO SERVIÇO

8.1. PRAZO

8.1.1. Início da execução do objeto: Imediatamente após a assinatura do contrato, seguindo o cronograma, conforme **Cronograma de realização dos serviços:**

8.1.1.1. O cronograma seguirá a seguinte estrutura:

8.1.1.1.1. Fase de Implantação: A Contratada deverá realizar a instalação dos equipamentos em até 60 dias após a assinatura do contrato.

8.1.1.1.2. Manutenção e suporte: Atendimento conforme SLA, conforme estipulado nos itens 5.3.16, 5.4.2 e 5.8.2.

8.1.1.1.3. Trocas e movimentações: com prazo de até 10 dias úteis para execução.

8.1.1.1.4. Relatórios Gerenciais: Entregues a pedido do Departamento de Tecnologia da Informação da Prefeitura.

8.2. LOCAL

8.2.1. Os serviços serão prestados no seguinte endereço: A Instalação do Item 1 deverá ocorrer no prédio da Secretaria Municipal de Administração – SMAD no Departamento de Tecnologia da Informação, sito à Rua Ramiro Barcelos, 2993. Centro. Montenegro/RS. E a Instalação do Item 2 deverá ocorrer no prédio da Secretaria Municipal de Saúde – SMS, sito à Rua Campos Neto, 177. Bairro Santa Rita. Montenegro/RS. Para os Itens 3 e 4, a instalação poderá ser feita remotamente mediante liberação dos técnicos do Departamento de Tecnologia da Informação.

8.3. HORÁRIO

8.3.1. Os serviços serão prestados no seguinte horário: As Instalações deverão ocorrer no período do expediente da Administração, salvo os acessos remotos que poderão ser agendados com a equipe técnica do Departamento de Tecnologia da Informação para horários diferentes. Demais serviços serão prestados 24x7 sem interrupções por conta de finais de semanas ou feriados.

9. OBRIGAÇÕES DA CONTRATANTE

9.1. São obrigações da Contratante:

9.1. Cumprir todas as suas obrigações constantes neste Termo de Referência e, ainda:

a) designar formalmente servidor público municipal para exercer o acompanhamento e a fiscalização do contrato;
b) acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através do servidor público municipal designado pela Secretaria;
c) prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA para a perfeita execução dos serviços;
d) agendar reuniões e/ou vistorias com a CONTRATADA sempre que julgar necessário;
e) verificar, minuciosamente, a conformidade do objeto recebido, provisoriamente, com as especificações constantes no Termo de Referência e da proposta, para fins de aceitação e recebimento definitivo;
f) cientificar a CONTRATADA sobre as normas internas vigentes relativas à segurança, inclusive aquelas atinentes ao controle de acesso de pessoas e veículos, bem assim sobre a Política de Segurança da Informação da CONTRATANTE;

g) permitir o acesso de representantes, prepostos ou empregados da CONTRATADA aos locais onde serão prestados os serviços, observadas as normas que disciplinam a segurança do patrimônio e das pessoas;
h) comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no serviço prestado, para que seja reparado ou corrigido;
i) proporcionar todas as condições para que a CONTRATADA possa desempenhar suas tarefas dentro das normas e condições contratuais;
j) zelar pela perfeita execução dos serviços contratados, devendo as falhas que porventura venham a ocorrer serem anotadas e sanadas;
k) recusar, com a devida justificativa, qualquer serviço executado fora das especificações constantes no contrato;
l) efetuar o pagamento devido pela execução dos serviços, desde que cumpridas todas as formalidades e exigências do contrato;
m) aplicar as penalidades previstas, contratualmente, após o contraditório e a ampla defesa, no caso de descumprimento de cláusulas contratuais pela CONTRATADA. OBSERVAÇÃO: O Município de Montenegro não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do objeto, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

10. OBRIGAÇÕES DA CONTRATADA

10.1. A Contratada deve cumprir todas as obrigações constantes neste Termo de Referência e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

a) responsabilizar-se pelos encargos sociais, taxas, encargos ou tributos, alvarás e qualquer outra despesa que vier a incidir sobre o serviço, bem como qualquer responsabilidade de vínculo empregatício e obrigações previdenciárias, referentes ao pessoal utilizado nos serviços, no caso de reclamações trabalhistas, ações de responsabilidade civil e penal decorrentes dos serviços de qualquer tipo de demanda, devendo atender o disposto na legislação trabalhista e previdenciária;
b) responsabilizar-se pelos materiais, mão de obra, equipamentos, ferramentas, utensílios, EPI's, insumos e transporte necessários à elaboração e impressão dos projetos, bem como encargos decorrentes da aprovação e licenciamento junto aos órgãos próprios para execução dos serviços contratados;
c) responsabilizar-se por qualquer acidente que venha a ocorrer com os empregados envolvidos na execução do contrato;
d) responsabilizar-se integralmente pelo objeto contratado, nas quantidades e padrões estabelecidos, vindo a responder pelos danos causados diretamente ao Município ou a terceiros, decorrentes de sua culpa ou dolo, especialmente no que se refere a prejuízos causados por erros quantitativos ou financeiros da planilha orçamentária elaborada pela CONTRATADA;
e) atender prazos, especificações técnicas, normas ambientais, de engenharia e de segurança e medicina do trabalho, além da legislação aplicável, assegurando sua conformidade, adequação, qualidade, segurança e solidez;
f) submeter-se às normas administrativas, operacionais e de segurança da CONTRATANTE;
g) manter e zelar pelos objetos e equipamentos que eventualmente sejam colocados à sua disposição pela CONTRATANTE, responsabilizando-se pela reposição ou recuperação dos mesmos;

h) manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, as condições de habilitação e qualificação exigidas na licitação;
i) indicar preposto para representá-la durante a execução dos serviços, se for o caso;
j) prestar todos os esclarecimentos solicitados pela CONTRATANTE, atendendo prontamente a todas as reclamações;
k) registrar via e-mail para o funcionário designado pela CONTRATANTE, todos os impedimentos que possam afetar o cronograma de trabalho;
l) manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da CONTRATANTE, ou de terceiros de que tomar conhecimento em razão da execução do objeto deste contrato, sobretudo no que se refere às condições médicas dos servidores públicos municipais;
m) fornecer e assegurar a utilização dos Equipamentos de Proteção Individual e Equipamentos de Proteção Coletiva necessários à proteção da integridade física dos seus trabalhadores, caso necessário;
n) recolher o documento de Responsabilidade Técnica emitido pela entidade de classe competente;
o) emitir as Notas Fiscais referentes ao valor das medições aprovadas pela fiscalização.

CAPÍTULO IV
DO MODELO DE GESTÃO DO CONTRATO

11. CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

11.1. Nos termos do art. 117, da Lei nº 14.133/2021, será designado representante para acompanhar e fiscalizar a entrega do objeto contratado, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

11.2. O fiscal informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência.

11.3. O fiscal poderá solicitar, a qualquer tempo, com fundamento em critérios objetivos, a substituição do profissional indicado pela CONTRATADA, caso não esteja desempenhando ou correspondendo nas funções determinadas.

11.4. O fiscal poderá ser auxiliado pelos órgãos de assessoramento jurídico e de controle interno da Administração, que deverão dirimir dúvidas e subsidiá-lo com informações relevantes para prevenir riscos na execução contratual.

11.5. O Gestor e o Fiscal do Contrato, e seus suplentes, serão designados em Portaria pela autoridade competente após a fase externa da licitação, no momento da elaboração e assinatura contratual.

11.5.1. Estão previamente indicados como Gestor do Contrato, o Secretário Responsável pela Pasta, e como Suplente, o seu eventual substituto.

11.5.2. Estão previamente indicados como Fiscal do Contrato, e seu Suplente, respectivamente, **Antonio Gonçalves de Oliveira Junior e Paulo Eduardo Lottermann.**

11.5.3. As substituições de Gestores e Fiscais de Contrato serão realizadas por apostilamento, as quais será dada a ciência a CONTRATADA mediante envio de e-mail ou outro meio de contato que tenha sido previamente disponibilizado pela CONTRATADA.

11.6. Os pormenores da designação e a forma de atuação dos Gestores e Fiscais do Contrato, derivado deste Termo de Referência, estão expressas no Anexo VI do Decreto Municipal n.º 9.555/2024.

12. DOS PROCEDIMENTOS DE TESTES E INSPEÇÕES (NA EMPRESA)

12.1. O CONTRATANTE reserva-se ao direito de promover avaliações, inspeções e diligências visando esclarecer quaisquer situações relacionadas a execução do objeto contratado, sendo obrigação da CONTRATADA acolhê-las.

CAPÍTULO V
DOS CRITÉRIOS DE RECEBIMENTO E PAGAMENTO

13. DOS CRITÉRIOS DE RECEBIMENTO

13.1. O objeto contratado será recebido provisoriamente pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta vencedora.

13.2. A entrega poderá ser rejeitada, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta vencedora, devendo ser substituídos no prazo definido de até 10 (dez) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

13.3. Após a prestação do serviço, o recebimento provisório deverá ocorrer em até 10 (dez) dias, que atestará a qualidade do bem ou serviço executado e consequente aceitação. Já o recebimento definitivo deverá ocorrer em até 10 (dez) dias após o aceite provisório.

13.3.1. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais, respeitadas as condições estabelecidas no item 2.3. deste Termo de Referência.

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

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

13.5. O recebimento provisório ou definitivo não exclui a responsabilidade civil pelo fornecimento do objeto licitado, nem a ético-profissional pela perfeita execução deste objeto.

14. DAS SANÇÕES ADMINISTRATIVAS

14.1. Comete infração administrativa nos termos do art. 155, da Lei nº 14.133/2021, a Contratada que:

a) dar causa à inexecução parcial do contrato;

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

c) dar causa à inexecução total do contrato;

d) deixar de entregar a documentação exigida para o certame;

e) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

f) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

g) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

h) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

i) fraudar a licitação ou praticar ato fraudulento na execução do contrato;

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

k) praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

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

15. DAS PENALIDADES

15.1. A recusa injusta da adjudicatária em assinar o contrato, entregar o objeto, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido pelo Município de Montenegro, caracteriza o descumprimento total da obrigação assumida, sujeitando-se às penalidades aqui previstas.

15.2. O Licitante que descumprir injustificadamente as regras do Edital, por sua participação em processo licitatório será penalizado com multa de 5% (cinco por cento) do valor estimado da contratação, sem prejuízo de aplicação de sanções previstas nos inc. III e IV, do § 1º, art. 155 da Lei n.º 14.133/2021.

15.3. Pela inexecução total ou parcial do objeto, a Administração pode aplicar à Contratada as seguintes sanções, de acordo com o art. 156, da Lei nº 14.133/2021:

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

b) multa monetária;

c) rescisão de contrato;

d) impedimento do direito de licitar junto ao Município de Montenegro;

e) declaração de inidoneidade para contratar ou transacionar com o Município de Montenegro.

15.4 Na aplicação das sanções serão considerados:

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para a Administração Pública;

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

15.5. Para aplicação das sanções, será observado o disposto no § 2° do art. 156 ao art. 163, da Lei nº 14.133/2021:

15.6. A critério da autoridade competente, a aplicação de quaisquer penalidades mencionadas no item 15.5. acarretará perda da garantia e todos os seus acréscimos.

15.7. Será aplicada multa de 0,5% (cinco décimos por cento) do valor total corrigido do contrato, por dia de atraso no fornecimento de materiais e serviços, até o limite de 60 dias.

15.8. Ultrapassado o período de tolerância previsto no subitem 15.7, ter-se-á como inexecutado o contrato.

15.9. A causa determinante da multa deverá ficar plenamente comprovada e o fato a punir, comunicado por escrito pela fiscalização ao gestor do contrato.

15.10. Será aplicada a sanção de impedimento de licitar e contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até 03 (três) anos ao responsável pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do caput do art. 155 da Lei n.º 14.133/2021;

15.11. Será aplicada a sanção de declaração de inidoneidade para licitar ou contratar com a Administração Pública, ao responsável pelas infrações administrativas previstas nos incisos VIII, IX,X, XI e XII do caput do art. 155 da Lei n.º 14.133/2021, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do caput do referido artigo que justifiquem a imposição de penalidade mais grave que a sanção referida no § 4º do art. 156 da mesma Lei, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos;

15.12. As sanções previstas nos incisos I, III e IV, do § 1º, art. 156 da Lei n.º 14.133/2021 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados

15.13. Quando o objeto do contrato não for entregue no todo ou parcialmente dentro dos prazos estipulados, a suspensão do direito de licitar será automática e perdurará até que seja feita a entrega do objeto do contrato na sua totalidade, sem prejuízo de outras penalidades previstas em lei e neste edital.

15.14. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei n.º 14.133/2021.

15.15. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor do Município, ou deduzidos da garantia, se houver, ou ainda, quando for o caso, serão inscritos na Dívida Ativa do Município e cobrados judicialmente.

15.15.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, após garantida a ampla defesa e o contraditório ao contratado.

PREFEITURA MUNICIPAL DE MONTENEGRO

15.16. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a Administração poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

16. DO PAGAMENTO.

16.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, a liquidação ocorrerá no prazo de até 20 (vinte) dias.

16.1.1. Para os fins de liquidação, deverá ser observado o disposto no art. 63 da Lei nº 4.320, de 17 de março de 1964, certificando-se do adimplemento da obrigação do contratado nos prazos e forma previstos no contrato.

16.1.2. Os prazos de que tratam os itens 16.1 e 16.2 do deste Termo de Referência poderão ser excepcionalmente prorrogados, justificadamente, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

16.1.3. O prazo previsto no item 13.2para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins de que tratam os itens 16.1 e 16.2.

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

16.1.4.1. Os dados do contrato, do órgão contratante e do contratado;

16.1.4.2. A data da emissão;

16.1.4.3. O prazo de validade;

16.1.4.4. O período respectivo de execução do contrato;

16.1.4.5. O valor a pagar;

16.1.4.6. Eventual destaque do valor de retenções tributárias cabíveis;

16.1.4.7. Número da Nota de Empenho;

16.1.4.8. Dados bancários para pagamento;

16.1.4.9. Identificação do Nome e Número do Convênio, quando houver utilização de recurso vinculado via convênio do Estado ou da União.

16.2. O pagamento será efetuado no prazo de até 20 (vinte) dias contados da liquidação da despesa.

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

16.2.1.1 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.

16.3. Na hipótese de caso fortuito ou força maior que impeça a liquidação ou o pagamento da despesa, o prazo para o pagamento será suspenso até a sua regularização, devendo ser mantida a posição da ordem cronológica que a despesa originalmente estava inscrita.

16.4. No caso de insuficiência de recursos financeiros disponíveis para quitação integral da obrigação, poderá haver pagamento parcial do crédito, permanecendo o saldo remanescente na mesma posição da ordem cronológica.

16.5. Previamente ao pagamento, a Administração deve verificar a manutenção das condições exigidas para a habilitação na licitação, ou para a qualificação, na contratação direta.

16.6. A eventual perda das condições de que trata o item 16.5 não enseja, por si, retenção de pagamento pela Administração.

16.7. Verificadas quaisquer irregularidades que impeçam o pagamento, a Administração deverá notificar o fornecedor contratado para que regularize a sua situação.

16.8. A permanência da condição de irregularidade, sem a devida justificativa ou com justificativa não aceita pela Administração, pode culminar em rescisão contratual, sem prejuízo da apuração de responsabilidade e da aplicação de penalidades cabíveis, observado o contraditório e a ampla defesa.

16.9. É facultada a retenção dos créditos decorrentes do contrato, até o limite dos prejuízos causados à Administração Pública e das multas aplicadas, nos termos do inciso IV do art. 139 da Lei nº 14.133, de 2021.

16.10. Em caso de atraso no pagamento, motivado exclusivamente pelo contratante, o valor devido será corrigido pelo INPC, apurados desde a data prevista para o pagamento até a data de sua efetiva realização.

16.11. 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.

17. DO REAJUSTAMENTO

17.1. Os preços são fixos, porém reajustáveis no prazo de um ano contado da data do orçamento estimado, adotando-se a seguinte regra:

17.1.1. Dentro do prazo de vigência do contrato, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice INPC/IBGE, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na seguinte fórmula:

$$R = V (I – I^o) / I^o, \text{ onde:}$$

R = Valor do reajuste procurado;
V = Valor contratual a ser reajustado;
Iº = índice inicial - refere-se ao índice de custos ou de preços correspondente à data do orçamento estimado pela Administração;

I = Índice relativo ao mês do reajustamento

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

17.3. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

17.4. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

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

17.6. 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.

17.7. O reajuste será realizado por apostilamento.

18. DOS CRITÉRIOS DE REDUÇÕES DE PAGAMENTO

18.1. Será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

a) Não produziu os resultados acordados;

b) Deixou de fornecer os itens contratados, ou não os entregou na qualidade mínima exigida o;

c) Deixou de utilizar os materiais e/ou recursos humanos exigidos para a entrega ou utilizou-os com qualidade ou quantidade inferior à demandada.

18.2. A aplicação de descontos/glosas em função do descumprimento de critérios de qualidade, avaliação de resultados e/ou níveis mínimos de serviço exigidos não concorre com a aplicação (concomitante ou não) das sanções administrativas previstas em CONTRATO, inclusive daquelas previstas em função do reiterado descumprimento dos critérios de qualidade dos produtos/serviços, sendo essa uma prerrogativa da Administração.

CAPÍTULO VI
FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

19. MODALIDADE E CRITÉRIO DE JULGAMENTO

MODALIDADE E CRITÉRIO DE JULGAMENTO

19.1. Considerando a natureza e os valores estimados do objeto a ser contratado, será licitado por meio de Pregão **a ser definida no processo preliminar**, com critério de julgamento Menor Preço nos termos da Lei 14.133/21.

19.2. Será selecionado o fornecedor que atender a todos os critérios de aceitabilidade de preços e de habilitação exigidos neste Termo de Referência.

PREFEITURA MUNICIPAL DE MONTENEGRO

20. CRITÉRIOS DE APRESENTAÇÃO E ACEITAÇÃO DA PROPOSTA

20.1. A proposta de preço deverá conter as seguintes indicações:

a) identificação do proponente (Razão Social/Nome e CNPJ/CPF);

b) a proposta financeira deverá ser formulada, contendo preço unitário por item, total por item e total geral, onde deverão estar incluídos, contabilizados e previstos todos os custos inerentes a execução do objeto, indicando, no que for aplicável, a marca, o modelo, prazo de validade ou de garantia; número do registro ou inscrição do bem no órgão competente, quando for o caso;

c) prazo de validade da proposta que deverá ser de no mínimo 60 (sessenta) dias;

d) apresentada a proposta, o proponente estará automaticamente aceitando e se sujeitando às cláusulas e condições do presente Termo de Referência;

e) assinatura do responsável legal da empresa.

f) A proponente deverá apresentar a proposta obrigatoriamente indicando marca, modelo, componentes, licenças, módulos e/ou acessórios necessários para a total e completa instalação de cada item ofertado, em conformidade com as características do Termo de Referência, sob pena de desclassificação.

g) A proponente deverá anexar, juntamente com a proposta, todos os catálogos, declarações e manuais necessários à comprovação técnica da solução ofertada, sob pena de desclassificação.

h) As soluções referentes aos lotes 1 a 4 deverão, obrigatoriamente, ser do mesmo fabricante, de modo a garantir a plena integração entre os componentes de segurança, tendo em vista que a integração total é premissa essencial deste projeto.

20.1.1. Serão considerados, para fins de julgamento, os valores constantes no preço até, no máximo, duas casas decimais após a vírgula, sendo desprezadas as demais, se houver, também em eventual contratação.

20.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

20.3 A solução ofertada deverá ser integrada, com capacidade de interoperabilidade entre seus componentes, permitindo a troca automatizada de informações de segurança. O fornecimento incluirá equipamento, software, licenças de proteção e gerenciamento para estações e servidores, contemplando a instalação, configuração e gerenciamento em nuvem, tanto para dispositivos pertencentes ao domínio quanto para aqueles externos.

20.4. A proposta também deverá contemplar treinamento da equipe técnica interna e suporte técnico contínuo durante toda a vigência contratual, conforme descrito no Estudo Técnico Preliminar e nos demais termos deste documento.

20.5. O preço proposto deverá ser completo abrangendo todos os tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais), mão de obra, prestação de serviço, fornecimento de mão de obra especializada, leis sociais, administração, lucros, equipamento e ferramental, transporte de material e de pessoal, translado, seguro do pessoal utilizado nos serviços contra riscos de acidente de trabalho, cumprimento de todas as obrigações que a legislação

trabalhista e previdenciária imposta ao empregador e qualquer despesa acessória e/ou necessária, não especificada neste Termo de Referência.

20.6. A análise das propostas visará ao atendimento das condições estabelecidas neste Termo de referência e seus anexos, sendo desclassificadas as propostas:

a) cujo objeto não atenda às especificações, prazos e condições fixadas neste Termo de Referência;
b) que apresentem preço excessivo ou manifestamente inexequível;
c) que no caso de exigência, não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita, ou havendo entrega de amostra fora das especificações previstas.

20.7. DOCUMENTO OFICIAL DO FABRICANTE

( ) Não (X) Sim

Deverá ser apresentado juntamente com a proposta comercial os catálogos, folders e demais comprovantes que comprovem os atendimentos das especificações técnicas dos equipamentos e softwares. Será aceito também declaração do fabricante comprovando os pontos que, por ventura, não estejam explícitos nos catálogos.

21. DOCUMENTAÇÃO EXIGIDA - CRITÉRIOS DE HABILITAÇÃO

21.1. Para fins de habilitação neste processo, o licitante deverá apresentar os seguintes documentos:

HABILITAÇÃO JURÍDICA

a) 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;
b) Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;
c) 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;
d) Sociedade empresária, sociedade limitada unipessoal – SLU ou Sociedade Limitada–LTDA: 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;
e) 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;
f) Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

g) 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;
h) 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;
i) Agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pela Secretaria Especial de Agricultura Familiar e do Desenvolvimento Agrário, nos termos do art. 2º, §3º do Decreto nº 11.802, de 28 de dezembro de 2023;
j) Produtor Rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB n. 2.110, de 17 de outubro de 2022(arts. 15 a 17 e 146);

Observação 1. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Observação 2. Independente do documento apresentado para cumprimento do disposto nos subitens do item 21.1, o objeto social da LICITANTE deve ser compatível com o objeto do presente certame.

REGULARIDADE FISCAL, SOCIAL E TRABALHISTA

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;
b) 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;
c) Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
d) 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;
e) Prova de inscrição no cadastro de contribuintes Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
f) Prova de regularidade com a Fazenda Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
g) Caso o fornecedor seja considerado isento dos tributos Municipal 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;
h) 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

PREFEITURA MUNICIPAL DE MONTENEGRO

Observação 3: Microempresas, Microempreendedor Individual e/ou Empresas de Pequeno Porte, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que está apresente alguma restrição (Lei Complementar n.º 123, de 14/12/06).

DECLARAÇÕES

a) Declaração que nos termos do art. 7º, XXXIII da CF/88, não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e de qualquer trabalhador menor de 16 anos, salvo na condição de aprendiz, a partir de 14 anos;
b) Declaração de que a empresa não foi considerada inidônea para licitar ou contratar com a Administração Pública e de que comunicará a ocorrência de fatos supervenientes impeditivos para a sua participação no presente processo licitatório;
c) Declaração de Inexistência de parentesco firmada pelo representante legal da empresa, nos termos da Lei 14.133/21;
d) Declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas;
e) Declaração de que atende os requisitos de habilitação;
f) Declaração que não possui inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pela Portaria Interministerial MTE/SDH n.º 4/2016 e não ter sido condenada, a contratada ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta a previsão aos artigos 1° e 170 da Constituição Federal de 1988; do artigo 149 do Código Penal; do Decreto n.º 5.017/2004 (promulga o Protocolo de Palermo) e das Convenções da OIT nos 29 e 105;
g) Declaração que os objetos são fornecidos por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei n. 8.213, de 24 de julho de 1991;
h) Declaração de que o licitante tomou conhecimento de todas as informações contidas neste Termo de Referência, e seus anexos, e das condições locais para o cumprimento das obrigações objeto da licitação;
i) Declaração que no ano-calendário, ainda não tenha celebrado com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, no caso de ME e EPP;
j) Declaração de integração das soluções, garantia de suporte e treinamento. Caso a licitante não seja a própria desenvolvedora, deverá a fabricante emitir documento em favor da licitante garantindo o pleno atendimento, **como condição para assinatura do contrato.**

Observação 4: Caso alguma das declarações acima já tenham sido prestadas como condição para participação do certame, não serão exigidas as suas apresentações.

QUALIFICAÇÃO ECONÔMICO- FINANCEIRA

Não se aplica.

PREFEITURA MUNICIPAL DE MONTENEGRO

QUALIFICAÇÃO TÉCNICA

(x) Sim () Não

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

a.1) Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

> ***a.1.1)*** fornecimento ou implantação de solução similar em ambiente de igual porte ou complexidade, incluindo **sistemas de firewall de última geração, gerenciamento em nuvem e integração com diretórios de autenticação (como Active Directory).**

a.2) *Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.*

a.3) *Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.*

a.4) *O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos*

b) declaração, de que, se vencedora, apresentará a relação do quadro técnico, **como condição para assinatura do contrato.**

21.2. A apresentação de documentos falsificados ou adulterados acarretará a emissão de declaração de inidoneidade e sujeitará a empresa as penalidades previstas no item 15.

21.3. Os documentos apresentados deverão conter, preferencialmente, assinatura com certificação digital no padrão da Infraestrutura de Chaves Públicas Brasileira – ICP Brasil.

21.4. Se a licitante for matriz, todos os documentos deverão estar em nome da matriz.

21.4.1. Se a licitante for filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos, que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

21.5. Os documentos que dependam de prazo de validade e que não contenham esse prazo especificado no próprio corpo, em lei ou neste processo, devem ter sido expedidos em no máximo 180 (cento e oitenta) dias anteriores a data determinada para a entrega da documentação.

21.6. São condições técnicas para **assinatura do contrato**:

a) **Caso a licitante vencedora não seja a própria desenvolvedora**, deverá a fabricante emitir documento em favor da licitante vencedora garantindo o pleno atendimento.

b) apresentar a relação do quadro técnico:

b.1) 1(um) profissional certificado em CompTIA Security+ ou CISSP.

b.2) 1 (um) profissional habilitado em Eng. Computação ou Eng. Telecom ou Eng. Elétrica.

22. ESTIMATIVA DE PREÇOS

22.1. O custo estimado total da contratação é de R$ 4.632.448,67, conforme custos unitários e totais apostos na tabela no Item 1.

22.1.1. Foram realizadas consultas a três fornecedores especializados (Domus Automação Ltda, Estratégia IT e Technoplus Serviços Ltda), selecionados em razão de sua reconhecida atuação no mercado de cibersegurança e da capacidade de ofertar soluções compatíveis com as especificações técnicas demandadas pelo Município. Na sequência, procedeu-se à verificação de contratações em portais públicos. Dentre as pesquisas realizadas, identificou-se, no sítio Portal de Compras Públicas, o Pregão Eletrônico nº 004/2025, do Município de Estrela. Entretanto, constatou-se pouca similaridade entre o objeto ali contratado e as necessidades descritas neste Termo de Referência, razão pela qual não foi possível utilizá-lo como parâmetro de pesquisa. Considerando que não foram encontradas soluções com características equivalentes — especificamente firewall de próxima geração com integração EDR e recursos avançados de Endpoint —, a pesquisa de preços ficou restrita a fornecedores privados, nos termos do art. 23, §1º, II, da Lei nº 14.133/2021. Cumpre destacar que, ainda que não tenham sido localizados itens idênticos em sistemas oficiais, a pesquisa foi conduzida de modo a assegurar representatividade e aderência às práticas de mercado, em consonância com o entendimento firmado pelo Tribunal de Contas da União no Acórdão nº 1712/2025.

22.1.2. Para fins da data-base para o reajustamento previsto no § 7º do art. 25 da Lei n.º 14.1333/2021, o orçamento estimado pela Administração foi realizado na data de 18/07/2025 em forma de Pesquisa Direta com Fornecedores através de e-mail utilizando-se do modelo da planilha abaixo, individualmente.

23. ADEQUAÇÃO ORÇAMENTÁRIA

23.1. Os recursos destinados à cobertura das despesas ora pretendidos se encontram alocados no Orçamento Geral do Município e serão custeadas com recursos financeiros provenientes do Tesouro Municipal.

23.2. A contratação será atendida pela seguinte dotação:

Unidade Gestora: *Secretaria de Administração*

Dotação:*2025/243*

Programa de Trabalho: *03.05.04.126.0221.2308*

Elemento de Despesa: *3.3.90.40.00.00.00.00 – Serviço de Tecnologia da Informação e Comunicação - PJ*

Fonte de Recurso: *1500 – Recursos não Vinculados de Impostos*

Rubrica do Item: *3.3.90.40.06.00.00.00 – Locação de Software*

PREFEITURA MUNICIPAL DE MONTENEGRO

Unidade Gestora: *Secretaria de Administração*

Dotação:*2025/243*

Programa de Trabalho: *03.05.04.126.0221.2308*

Elemento de Despesa: *3.3.90.40.00.00.00.00 – Serviço de Tecnologia da Informação e Comunicação - PJ*

Fonte de Recurso: *1500 – Recursos não Vinculados de Impostos*

Rubrica do Item: *3.3.90.40.20.00.00.00 – Treinamento/Capacitação em T.I.C*

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

CAPÍTULO VII
DISPOSIÇÕES GERAIS E INFORMAÇÕES COMPLEMENTARES

24.1 Estão vinculados a este Termo de Referência:

I. Documento de Formalização de Demanda
II. Estudo Técnico Preliminar;

Montenegro, 31 de julho de 2025.

Antonio Gonçalves de Oliveira Junior

Técnico de Suporte em Informática

Ingrid Lerch

Secretário Municipal de Administração