PREGÃO ELETRÔNICO Nº 098/2026

***SECRETARIA**: SECRETARIA MUNICIPAL DE INOVAÇÃO E EMPREENDEDORISMO*
***SOLICITAÇÃO Nº** 2026/3523;*
***DATA:** 08 DE OUTUBRO DE 2026*
***HORA:** 08 HORAS E 30 MINUTOS*
***OBJETO**: CONTRATAÇÃO DE EMPRESA PARA A PRESTAÇÃO DE SERVIÇO DE LOCAÇÃO DE "APPLIANCE DE FIREWALL NEXT GENERATION" - NGFW*
***CRITÉRIO DE JULGAMENTO:** MENOR PREÇO POR LOTE*
***REGIME:** SERVIÇO ESPORÁDICO SEM DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA*
***PARTICIPAÇÃO:** GLOBAL*
***MODO DE DISPUTA:** ABERTO*

O **MUNICÍPIO DE GARIBALDI** torna público, para conhecimento dos interessados, que, no dia e hora acima descritos, realizará licitação na modalidade pregão, na forma eletrônica, do tipo menor preço, através do endereço eletrônico www.pregaobanrisul.com.br, processando-se essa licitação nos termos da Lei Federal nº 14.133 de 1º de abril de 2021, da Lei Complementar nº 123, de 14 de dezembro de 2006, IN nº 73 de 2022 e do Decreto Municipal nº 4.765/2023.

Maiores informações encontram-se à disposição dos interessados na Prefeitura Municipal de Garibaldi, RS, junto ao Departamento de Compras e Licitações, localizado na Rua Júlio de Castilhos, nº 254, Centro, ou pelo telefone (54) 3462-8228, ou ainda através do e-mail: licitacoes@garibaldi.rs.gov.br.

As empresas que desejarem participar do referido PREGÃO ELETRÔNICO deverão efetuar os procedimentos junto ao sítio eletrônico, conforme determinado neste edital.

1- DO OBJETO

1.1. A presente licitação tem por objeto a contratação de empresa especializada para a locação de solução de Firewall de Próxima Geração (Next Generation Firewall – NGFW), por meio de appliance em hardware dedicado, incluindo o fornecimento dos equipamentos, licenciamento integral de todas as funcionalidades, instalação, configuração, migração da solução atualmente em operação, suporte técnico especializado, garantia, manutenção corretiva, atualização de firmware e de assinaturas de segurança, bem como todos os demais serviços necessários ao pleno funcionamento da solução durante toda a vigência contratual, nos termos das tabelas abaixo, conforme condições e exigências estabelecidas neste edital.

LOTE ÚNICO					
ITEM	**OBJETO**	**QTDE**	**UN**	**VALOR UNITÁRIO**	**VALOR TOTAL**
01	SERVIÇOS DE LOCAÇÃO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL – NGFW), COMPREENDENDO O FORNECIMENTO DE APPLIANCE EM HARDWARE DEDICADO, LICENCIAMENTO COMPLETO DE TODAS AS FUNCIONALIDADES DE SEGURANÇA, SUPORTE TÉCNICO, GARANTIA, ATUALIZAÇÕES DE FIRMWARE, ASSINATURAS DE SEGURANÇA (IPS, ANTIVÍRUS, ANTIMALWARE, FILTRO DE CONTEÚDO WEB, CONTROLE DE APLICAÇÕES E WEB APPLICATION FIREWALL – WAF), ALÉM DO SERVIÇO DE LOGGING	12	UN	R$ 7.240,66	R$ 86.887,92

	ANALYTICS PARA ARMAZENAMENTO, PROCESSAMENTO E ANÁLISE DOS REGISTROS (LOGS) GERADOS PELO EQUIPAMENTO. 10GB/DIA				
02	IMPLEMENTAÇÃO	01	UN	R$ 23.307,47	R$ 23.307,47
VALOR TOTAL DO LOTE R$ 110.195,39					

1.2. A solução de NGFW a ser fornecida através de "*appliance"* com capacidade de Inspeção profunda de pacotes (DPI), análise detalhada do tráfego para identificar ameaças ocultas, prevenção contra intrusões (IPS/IDS) e bloqueio proativo de tentativas de exploração de vulnerabilidades, além de oferecer a possibilidade de auditoria dos acessos realizados através da emissão e gestão de relatórios especializados.

1.3. A solução deverá atuar como principal mecanismo de proteção do perímetro da rede corporativa e da rede interna da Administração Municipal, realizando inspeção, monitoramento e controle de todo o tráfego de dados entre a rede interna e a Internet, bem como entre segmentos internos da infraestrutura tecnológica, prevenindo acessos não autorizados, ataques cibernéticos e demais ameaças que possamcomprometer a disponibilidade, integridade e confidencialidade das informações.

1.4. A solução deverá contemplar, no mínimo, funcionalidades de Firewall Stateful, inspeção profunda de pacotes (Deep Packet Inspection – DPI), controle de aplicações por camada 7 (Layer 7), identificação de usuários, administração de largura de banda (QoS), VPN IPsec, Sistema de Prevenção e Detecção de Intrusão (IPS/IDS), proteção contra vírus, malwares e demais códigos maliciosos, filtro de conteúdo web, inspeção de tráfego criptografado (SSL Inspection), proteção de aplicações web (Web Application Firewall – WAF), geração de relatórios especializados e mecanismos avançados de auditoria dos acessos realizados.

1.5. A solução deverá incluir serviço de Logging Analytics, responsável pelo armazenamento, indexação, pesquisa e análise dos registros de eventos (logs) gerados pelo equipamento, permitindo a rastreabilidade das ações realizadas na rede, emissão de relatórios gerenciais, auditoria de eventos de segurança e apoio às atividades de monitoramento e resposta a incidentes. A capacidade mínima contratada deverá ser de 10 GB de ingestão de logs por dia, atendendo ao consumo atual da infraestrutura municipal e prevendo margem para o crescimento da demanda durante a vigência contratual.

1.6. Também deverão integrar a contratação todas as licenças necessárias ao funcionamento integral da solução, incluindo atualizações de firmware, assinaturas de antivírus, antimalware, IPS, filtro de conteúdo web, controle de aplicações, Web Application Firewall (WAF) e demais componentes de segurança, sem qualquer custo adicional para a Administração durante todo o período da locação.

1.7. A contratada será responsável pela instalação física e lógica da solução, configuração dos equipamentos, migração das políticas de segurança atualmente existentes, integração com o ambiente de auditoria e gerenciamento de logs já implantado pelo Município, realização de testes de funcionamento, homologação da solução, treinamento operacional da equipe técnica e prestação de suporte técnico especializado durante toda a vigência do contrato.

1.8. A solução deverá ser compatível com instalação em rack padrão de 19 polegadas, conforme norma EIA-310, ocupando no máximo 1U de altura, e deverá garantir níveis adequados de desempenho para suportar o volume de tráfego da rede municipal, assegurando a continuidade dos serviços públicos digitais e permitindo futuras expansões da infraestrutura tecnológica sem necessidade de substituição prematura da solução contratada.

1.9. Por se tratar de uma solução integrada de hardware, software, licenciamento e serviços especializados, todos os componentes deverão ser fornecidos por uma única contratada, garantindo total compatibilidade entre os equipamentos, funcionalidades e serviços prestados, bem como maior eficiência na gestão contratual, na manutenção da solução e na responsabilização técnica durante toda a execução do contrato.

1.10. Fornecimento de solução de NGFW com as seguintes características:

1.10.1. CARACTERÍSTICAS DO HARDWARE:

• O equipamento deve ser compatível com instalação em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45 mm);

• Dispor de pelo menos duas fontes de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz cada;

• Possuir painel ou led indicador on/off e devices de rede;

• Possuir throughput de no mínimo 26 Gbps para tráfego UDP independente do tamanho dos pacotes;

• Suportar no mínimo 2.900.000 (dois milhões e novecentas mil) conexões simultâneas;

• Suportar no mínimo 130.000 (cento e trinta mil) novas conexões por segundo;

• Possuir throughput mínimo de 5 Gbps para tráfego IPS/IDS;

• Possuir throughput mínimo de 30Gbps para tráfego VPN IPSEC;

• Possuir throughput mínimo de 3 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

• Possuir pelo menos 16 (dezesseis) interfaces de rede Gigabit Ethernet 10/100/1000, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

• Possuir no mínimo 4 lans 10GBE SFP+;

• Possuir no mínimo 8 lans 1GBE SFP;

• Possuir no mínimo 1 (uma) porta console de conexão para acesso à interface de comando CLI específica para esta finalidade;

• Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos.

1.10.2. ESPECIFICAÇÃO GERAL DO SOFTWARE NGFW:

1.10.2.1. FUNÇÕES BÁSICAS

• Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;

• Agentless VPN, VPN ipsec (Client-to-site e Site-to-site);

• Controle de Aplicações;

• Proxy Web e Filtro de Conteúdo Web (URL Filtering);

• Detecção e prevenção de intrusos – IPS;

• Qualidade de serviço – QoS;

• Anti-Malware;

• SD-WAN;

• Cluster.

1.10.2.2. CARACTERÍSTICAS GERAIS

• Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui *stateful firewall* 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, IPS, prevenção contra ameaças de vírus, malwares, filtro de URL, inspeção de tráfego criptografado e proteção de firewall de aplicação Web.

• Interface em português e inglês;

• O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

• Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução;

• A solução deverá ser em hardware dedicado tipo *appliance* com sistema operacional customizado para garantir segurança e melhor desempenho;

• Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;

• Não deve ser necessária a instalação de qualquer software no dispositivo cliente para realizar o acesso ou a administração dos recursos do equipamento, bem como adição e utilização de

servidores e/ou appliances.

1.10.2.3. FUNCIONALIDADES DO FIREWALL

• Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;

• Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

• Deve possuir ferramentas para realizar backups de forma remota, por SSH, FTP, NFS ou próprio do fabricante. Deve também permitir backup em Pen-drive. A solução deve permitir o agendamento diário ou semanal do backup;

• Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.

• Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica;

• As cópias de segurança devem ser salvas criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

• Deve permitir habilitar ou desabilitar o registro de log por política de firewall.

• Possuir controle de acesso à internet por endereço IP de origem e destino;

• Possuir controle de acesso à internet por sub-rede;

• Possuir suporte a tags de VLAN (802.1q);

• Suportar agregação de links, segundo padrão IEEE 802.3ad;

• Possuir ferramenta de diagnóstico do tipo pcap;

• Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;

• Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

• Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.

• Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

• Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;

• Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.

• Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;

• Possuir funcionalidades de DHCP Cliente, Servidor e Relay;

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

• Possuir tecnologia de firewall do tipo Stateful;

• Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo/passivo e ativo/ativo;

• Permitir o funcionamento em modo transparente tipo "bridge";

• Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;

• Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);

• Deverá suportar forwarding de multicast;

• Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP e UDP;

• Permitir o agrupamento de serviços;

• Permitir o filtro de pacotes sem a utilização de NAT;

• Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

• Possuir mecanismo de anti-spoofing;

• Permitir criação de regras definidas pelo usuário;

• Permitir o serviço de autenticação para HTTP e FTP;

• Possuir a funcionalidade de balanceamento e contingência de links;

• 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.

• Deve dar suporte e ter licenciada a virtualização de firewall, permitindo a criação de, no mínimo, 5 (cinco) firewalls virtuais (contextos ou domínios virtuais), onde cada um possa assumir logicamente em modo de NGFW e ainda possibilitar o uso de interfaces de redes, endereçamentos, políticas e roteamentos distintos.

• Todas as funcionalidades devem estar disponíveis em todos os contextos, não havendo limitações de uso quando sendo apenas o firewall base ou seus contextos virtualizados.

• Deve permitir a criação de administradores independentes, para cada um dos firewalls virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que possam ser administrados por equipes distintas.

1.10.2.4. IDENTIFICAÇÃO DO USUÁRIO

• Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;

• 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;

• 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;

• A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

• 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;

• A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;

1.10.2.5. FUNCIONALIDADE DE REDE VIRTUAL PRIVADA (VPN)

• VPN baseada em appliance;
• Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
• Suporte a certificados PKI X.509 para construção de vpns;
• Possuir suporte a vpns ipsec site-to-site:
• Criptografia, 3DES, AES128, AES256, AES-GCM-128
• Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
• Algoritmo Internet Key Exchange (IKE) versões I e II;
• AES 128 e 256 (Advanced Encryption Standard);
• Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14;
• Deve permitir a arquitetura de vpn hub and spoke;
• Suporte a vpns ipsec client-to-site;

• Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);

• Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicosentre múltiplos dispositivos (spokes) com um gateway centralizador (hub).

1.10.2.6. FUNCIONALIDADE DO SISTEMA DE DETECÇÃO DE INTRUSÃO - IPS/IDS

• A Detecção de Intrusão deverá ser baseada em appliance;
• Possuir no mínimo 7.000 assinaturas ou regras de IPS/IDS;
• O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
• Possuir tecnologia de detecção baseada em assinatura;

• Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo bypass;

• O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;

• Possuir opção para administrar as listas de Blacklist, Whitelist e Quarentena com suporte a endereços ipv6;

• 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;

• Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (dos) do tipo Flood, Prot Scan e Sweep;

• Mecanismos de detecção/proteção de ataques;

• Reconhecimento de padrões;

• Análise de protocolos;

• Detecção de anomalias;

• Detecção de ataques de RPC (Remote procedure call);

• Proteção contra ataques de Windows ou netbios;

• Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

• Proteção contra ataques DNS (Domain Name System);

• Proteção contra ataques a FTP, SSH , Telnet e rlogin;

• Proteção contra ataques de ICMP (Internet Control Message Protocol);

• Alertas via correio eletrônico;

• 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;

• Capacidade de resposta ativa a ataques;

• Terminação de sessões via TCP resets;

• Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

• O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;

• Possuir filtros de ataques por anomalias;

• Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

• Permitir filtros de anomalias de protocolos;

• Suportar reconhecimento de ataques de dos, reconnaissance, exploits e evasion;

• Suportar verificação de ataque nas camadas de aplicação;

1.10.2.7. FUNCIONALIDADE DE QoS

• Adotar solução de Qualidade de Serviço baseada em appliance;

• 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;

• Permitir modificação de valores DSCP;

• Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;

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

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

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

• Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;

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

1.10.2.8. FUNCIONALIDADE DO ANTIVÍRUS

• Possuir funções de Antivírus, Anti-spyware;
• Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;
• Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);
• Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

1.10.2.9. FUNCIONALIDADE DO PROXY E FILTRO DE CONTEÚDO

• Possuir solução de filtro de conteúdo web integrado a solução de segurança;
• Possuir pelo menos 85 categorias para classificação de sites web;
• Possuir base mínima contendo, 1 milhão de sites internet web já registrados e classificados;
• 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;
• Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
• Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;
• Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;
• Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;
• Possibilitar a integração com servidores de cache WEB externos;
• Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®;
• 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;
• Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
• Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
• 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;
• Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
• Permitir a criação de listas personalizadas de urls permitidas – lista branca e bloqueadas – lista negra;
• Deverá permitir o bloqueio de urls inválidas cujo campo CN do certificado SSL não contém um domínio válido;
• Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
• Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
• Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
• Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
• Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
• Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e urls originadas de Spam;
• Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;
• Deverá permitir configurar a porta do Proxy Explícito.

1.10.2.10. FUNCIONALIDADE DO CONTROLE DE APLICAÇÕES

• As funcionalidades abaixo devem ser baseadas em Appliance:

• Reconhecer pelo menos 3.000 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/Video ou Audio, proxy ou tunelamento, mensagens instantâneas ou colaboração, compartilhamento de arquivos/storage, backup, mail;

• Reconhecer pelo menos as seguintes aplicações: 4Shared, Active Directory/SMB, Citrix ICA, DHCP Protocol, 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;

• 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, Vídeo Streaming/Play, Upload);

• Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

• 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, port hopping e túnel através de tráfego SSL encriptado;

• Atualizar a base de assinaturas de aplicações automaticamente;

• Reconhecer aplicações em ipv6;

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

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

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

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

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

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

• Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;

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

1.10.2.11. SISTEMA DE PROTEÇÃO ACANÇADA CONTRA AMEAÇAS - ATP

• Possuir sistema de proteção avançada contra ameaças (ATP) nativo;

• 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;

• 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;

• A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;

• Deve permitir a identificação de aplicativos e ameaças independente das portas e protocolos;

• 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;

• Deve permitir a atualização automática das assinaturas por meio de agendamento diário;

• Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, ataques P2P, trojans, worms, malwares para mobile, blacklist, vulnerabilidades conhecidas;

• Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;

• Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, ataques P2P, trojans, worms, malwares para mobile, blacklist, vulnerabilidades conhecidas;

• Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de voip tais como: Hotline, SIP, Skype;

• 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;

• Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: bittorrent, Gnutella, Napster e de Storages, tais como: Dropbox, Google Drive, Mega e onedrive;

• Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

• Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;

• Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as "ameaças detectadas" e as "ameaças bloqueadas";

• Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "aplicativos detectados" e os "aplicativos bloqueados";

• Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";

• 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.

1.10.2.12. SD-WAN (GERÊNCIA DE WAN)

• 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;

• Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;

• Permitir utilizar VPN ipsec para interligar unidades remotas;

• Possuir recurso de "persistência de link" para impedir a queda de conexões em aplicações que não suportam o load balance de link;

• 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;

• Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos relacionado ao recurso SD-WAN;

• Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações: Consumo de banda; Perda de pacotes; Jitter; Latência.

1.10.2.13. ALTA DISPONIBILIDADE

• Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Passivo ou Ativo/Ativo, com as implementações de Fail Over;

• 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;

• O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat.

1.10.2.14. REDUNDÂNCIA PARA MÚLTIPLOS ISPs (Provedores)

• A solução proposta deve suportar o balanceamento de carga e redundância para pelo menos 2 (dois) links de Internet;

• A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação;

• A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP;

• A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway;

• A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego ipv4 e ipv6.

1.10.3. FERRAMENTA DE GESTÃO DE RELATÓRIOS

1.10.3.1. CARACTERÍSTICA DA FERRAMENTA

• Deve ser do tipo appliance virtual (VM)
• Possuir capacidade de recebimento de logs de pelo menos 10 mil dispositivos
• Possuir a capacidade de receber pelo menos 9 Gbits de logs diários
• Deverá ser compatível com ambiente VMware ESXi 6.5 e superior
• Deverá ser compatível com ambiente Microsoft Hyper-V 2016, 2019 e 2022
• Deverá ser compatível com ambiente Citrix XenServer 8.2 e superior e Open Source Xen 4.2.5
• Deverá ser compatível com ambiente KVM
• Deverá ser compatível com ambiente Nutanix AHV
• Deverá ser compatível com ambiente Amazon Web Services (AWS)
• Deverá ser compatível com ambiente Microsoft Azure.
• Deverá ser compatível com o ambiente Google Cloud (GCP)
• Deverá ser compatível com o ambiente Oracle Cloud Infrastructure (OCI)
• Deverá ser compatível com o ambiente Alibaba Cloud (AliCloud)
• Não deve possuir limite na quantidade de múltiplas vCPU
• Não deve possuir limite para suporte a expansão de memória RAM

1.10.3.2. REQUISITOS MÍNIMOS DE FUNCIONALIDADE

• Suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções

• Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento.

• Permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento.

• Suportar SNMP versão 2 e 3

• Permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.

• Permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.

• Permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH

• Possuir autenticação de usuários para acesso à plataforma via LDAP
• Possuir autenticação de usuários para acesso à plataforma via Radius
• Possuir autenticação de usuários para acesso à plataforma via TACACS +
• Possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico
• Possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas.
• Possuir geração de relatórios de tráfego em tempo real, em formato de gráfico

• Possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.

• Possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP,

usuário e senha.

- Possuir visualização da quantidade de logs enviados de cada dispositivo monitorado
- Possuir mecanismos de apagamento automático para logs antigos.
- Permitir importação e exportação de relatórios
- Deve ter a capacidade de criar relatórios no formato HTML
- Deve ter a capacidade de criar relatórios em formato PDF
- Deve ter a capacidade de criar relatórios no formato XML
- Deve ter a capacidade de criar relatórios no formato CSV
- Deve permitir exportar os logs no formato CSV
- Deve gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.
- Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.
- A solução deve ter relatórios predefinidos
- Deve poder enviar automaticamente os logs para um servidor FTP externo para a solução
- A duplicação de relatórios existentes deve ser possível para edição posterior.
- Ter a capacidade de personalizar a capa dos relatórios obtidos.
- Permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.
- Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados.
- Ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas
- Deve ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real.
- Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo.
- Ter a capacidade de gerar e enviar relatórios periódicos automaticamente.
- Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.
- Permitir o envio por e-mail relatórios automaticamente.
- Deve permitir que o relatório seja enviado por email ao destinatário específico.
- Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.
- É necessário exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.
- Deve permitir o uso de filtros nos relatórios.
- Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.
- Permitir especificar o idioma dos relatórios criados
- Gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.
- Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.
- Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.
- Possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros.
- Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.
- Importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.

• Deve ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.
• Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.
• Deve ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.
• Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos
• Deve permitir visualizar em tempo real os logs recebidos.
• Deve permitir o encaminhamento de log no formato syslog.
• Deve permitir o encaminhamento de log no formato CEF (Common Event Format).
• Deve disponibilizar painel de operações SOC composto por widgets configuráveis, permitindo o monitoramento de eventos de segurança, ameaças, usuários, aplicações, tráfego de rede, VPN, redes sem fio, endpoints, indicadores operacionais da plataforma e demais informações provenientes dos dispositivos integrados, conforme as funcionalidades suportadas pela solução
• Suportar a configuração Master / Slave de alta disponibilidade na camada 3
• Gerar alertas de eventos a partir de logs recebidos
• Permitir a criação de incidentes a partir de alertas de eventos para o terminal
• Permitir a integração ao sistema de tickets do ServiceNow
• Incluir serviço Indicadores de Comprometimento (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredicto (classificação geral da ameaça), o número de ameaças detectadas.
• Deve permitir o suporte a logs na nuvem pública do Amazon S3
• Deve permitir o suporte a logs na nuvem pública do Microsoft Azure
• Permitir o suporte aos registros de nuvem pública do Gooogle Cloud
• Suportar o padrão SAML para autenticação do usuário administrador
• Relatórios de Firewall
• Deve ter um relatório de conformidade com o PCI DSS
• Possuir um relatório de uso do aplicativo SaaS
• Possuir um relatório de prevenção de perda de dados (DLP)
• Possuir um relatório de VPN
• Possuir um relatório IPS (Intruder Prevention System)
• Possuir um relatório de reputação do cliente
• Possuir um relatório de análise de segurança do usuário
• Possuir um relatório de análise de ameaças cibernéticas
• Possuir um breve relatório resumido diário de eventos e incidentes de segurança
• Possuir um relatório de tráfego DNS
• Possuir um relatório de tráfego de e-mail
• Possuir um relatório dos 10 principais aplicativos usados na rede
• Possuir um relatório dos 10 principais sites usados na rede
• Possuir um relatório de uso de mídia social

1.11. ACORDO DE NÍVEL DE SERVIÇO - SLA

1.11.1. A LICITANTE deverá providenciar os atendimentos dentro das regras estabelecidas nesta seção:

• suporte técnico prestado em horário comercial, de segunda a sexta-feira com os seguintes prazos:

a) o atendimento virtual (remoto) de até 30 minutos após a abertura do chamado;

b) o atendimento presencial (quando necessário) em até 04 horas úteis após a abertura do chamado;

1.12. SUPORTE TÉCNICO

1.12.1. A licitante deverá prover suporte técnico necessário para garantir o perfeito funcionamento da solução descrita neste termo, bem como zelar pela resolução de possíveis incidentes no nível de serviço exigido, visando a não interrupção dos serviços contratados.

1.12.2. A empresa licitante deverá fornecer no mínimo dois canais de suporte ao cliente, sendo ao menos um canal por via digital, sendo aceito sistema web, formulário em site, atendimento via Whatsapp ou outros similares, desde que, possuam a capacidade de registrar e emitir comprovante de abertura de chamado;

1.12.3. Toda solicitação de suporte emitida pela Prefeitura de Garibaldi deverá ser registrada e controlada através da Central de Suporte da licitante contendo, minimamente, os dados de data e horário da abertura do chamado, identificação do solicitante e do técnico que receberá o chamado para iniciar o atendimento.

1.12.4. Os custos de Suporte Técnico deverão estar incluídos e distribuídos nos preços unitários.

1.12.5. Serão consideradas como Suporte Técnico todas as atividades empreendidas pela licitante necessárias para assegurar o funcionamento dos equipamentos, com o objetivo de possibilitar a continuidade dos serviços instalados e de garantir a alta disponibilidade objetiva.

1.12.6. O Suporte Técnico deverá ser acionável e realizado de segunda a sexta, no horário das 08:00 às 11:30 horas e das 13:30 às 17:00 horas, compreendendo:

a) manutenção corretiva: série de procedimentos destinados a reparar e a corrigir os componentes dos equipamentos e serviços, sem ônus à Prefeitura de Garibaldi, mantendo seu pleno estado de funcionamento, removendo definitivamente os defeitos eventualmente apresentados;

b) manutenção adaptativa: série de procedimentos destinados a adequar os itens de configuração em razão de alterações no ambiente tecnológico que suporta os equipamentos e serviços devendo a licitante informar à Prefeitura de Garibaldi a necessidade de atualização de qualquer software relativo à solução de NGFW;

c) A sede/filial da licitante deverá estar localizada a no máximo 130 quilômetros do Centro Administrativo da prefeitura, viabilizando o prazo de atendimento presencial;

1.13. IMPLANTAÇÃO

1.13.1. A solução de NGFW atualmente existente no município é do fabricante FORTINET, utilizando o hardware "Fortigate 80F" com firmware na versão 7.4.12, o sistema de auditoria e gestão de relatórios está configurado em ambiente virtual, utilizando a plataforma Hyper-V da Microsoft;

1.13.2. O processo de implantação tem por objetivo a inserção do hardware e software na infraestrutura da PREFEITURA de forma que o resultado final seja uma solução de NGFW com as mesmas características de organização interna (regras de firewall, conexões com AD, interfaceamento, VLANS, etc.) da solução atual;

1.13.3. A PREFEITURA designará um profissional responsável para acompanhamento e fornecimento de todas as informações pertinentes à implantação;

1.13.4. Todas as atividades relativas à implantação deverão acontecer em dias úteis (SEGUNDA-SEXTA) no intervalo das 08:00 – 17:00hs, remotamente ou presencialmente, de acordo com a necessidade;

1.13.5. A LICITANTE deverá fornecer um plano de implantação contendo minimamente as etapas e prazos para ser atingidos até a conclusão da implantação e início da prestação do serviço. Este plano deverá ser submetido ao Departamento de T.I do município para avaliação e posterior liberação para início dos trabalhos de implantação;

1.13.5.1. Em caso da solução de NGFW ser do mesmo fabricante da solução atual do município, a LICITANTE poderá substituir o plano de implantação por acesso prévio à nova solução para avaliar a migração direta das configurações através da cópia/restauração do arquivo de configuração;

1.13.6. A solução a ser adquirida deverá ser configurada de maneira que não seja necessário aquisição de novo hardware ou software para o seu pleno funcionamento;

1.13.7. A solução a ser adquirida deverá ser configurada de maneira que não seja necessário alterações estruturais no formato de organização da floresta/domínio do Active Directory pertencente ao município de Garibaldi;

1.13.8. A LICITANTE deverá fornecer credenciais com permissões suficientes para que os técnicos do Município de Garibaldi consigam fazer o gerenciamento COMPLETO da solução, incluindo todas as áreas abrangentes ao funcionamento e layout de conexão, criação e alteração de usuários administradores;

1.14. O prazo de início será a partir da assinatura do contrato, momento a partir do qual a contratada estará autorizada a realizar a instalação, configuração e ativação dos serviços contratados.

1.15. Deverão ser fornecidos todo hardware e licenças para uso e atualização de todos os componentes de software, vacinas de antivírus/malwares, assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período vigente da locação;

1.16. Para os itens que representem bens materiais, a LICITANTE deverá fornecer produtos novos, sem uso anterior. Por cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento;

1.17. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-ofsale, 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;

1.18. Toda solução fornecida deverá estar coberta por danos causados por eventos de força maior, com origem elétrica ou do meio ambiente, devendo ser imediatamente substituído sem custos adicionais ao CONTRATANTE;

1.19. O prazo de entrega e ativação da solução é de 30 (trinta) dias corridos contados da data de emissão da ordem de compra;

1.20. A solução deverá ser entregue e configurada na Prefeitura Municipal de Garibaldi, localizada na Rua Júlio de Castilhos, 254, Bairro Centro, Garibaldi/RS.

1.21. O prazo de vigência da contratação será de até 12 (doze) meses, a contar da assinatura do contrato, podendo ser prorrogado sucessivamente por meio de Termo Aditivo, até atingir o limite máximo de 10 anos de vigência, nos limites do artigo 107 da Lei 14.133/2021, a critério da Secretaria Contratante.

1.22. Caso haja algum serviço em desacordo com as especificações constantes no Termo de Referência e na proposta ou que seja de péssima qualidade, deverão ser reparados no prazo de 15 (quinze) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades. Neste caso, a nota fiscal será retida até que seja regularizada a pendência, sendo autorizado o pagamento após a liberação da pessoa responsável.

2 – DA DIVULGAÇÃO DO EDITAL

2.1. O edital será publicado, no sitio eletrônico, no máximo, até o dia 24 de setembro de 2026;

2.2. A data e hora limite para recebimento de propostas nos termos exigidos no edital é 08 de outubro de 2026, às 08h29min;

2.3. A abertura das propostas ocorrerá no dia 08 de outubro de 2026, às 08hrs30min;

2.4. A disputa terá início no dia 08 de outubro de 2026, às 09hrs;

2.5. O endereço eletrônico para formalização de questionamentos e impugnações: licitacoes@garibaldi.rs.gov.br;

2.6. Sítio eletrônico da sessão: www.pregaobanrisul.com.br.

2.7. Todas as referências de tempo deste certame observarão obrigatoriamente o horário de Brasília – DF.

3 – DO CREDENCIAMENTO E DA PARTICIPAÇÃO DO CERTAME

3.1. Para participar do certame, o licitante deve providenciar o seu credenciamento, com atribuição de chave e senha, diretamente junto ao provedor do sistema, onde deverá buscar informações a respeito do seu funcionamento, regulamento e instruções para a sua correta utilização.

3.2. As instruções para o credenciamento podem ser acessadas no seguinte sítio eletrônico: www.pregaobanrisul.com.br, e pelo telefone (51) 3288-1160.

3.3.É de responsabilidade do licitante, além de se credenciar previamente no sistema eletrônico utilizado no certame, cumprir as regras do presente edital, devendo:

3.3.1. Responsabilizar-se formalmente pelas transações efetuadas em seu nome, assumir como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

3.3.2. Acompanhar as operações no sistema eletrônico durante o processo licitatório e responsabilizar-se pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pelo sistema ou de sua desconexão.

3.3.3. As informações acerca do andamento do processo licitatório serão encaminhadas pela Pregoeira, via chat, ficando a cargo do licitante a responsabilidade pelo acompanhamento.

3.3.4. Utilizar a chave de identificação e a senha de acesso para participar do pregão na forma eletrônica.

3.3.5. Solicitar o cancelamento da chave de identificação ou da senha de acesso por interesse próprio.

3.4. Não poderão disputar licitação ou participar da execução do contrato, direta ou indiretamente:

a) pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

b) aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

c) empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

d) pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

e) agente público do órgão licitante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria;

f) aquele que não atenda às condições deste Edital e seu(s) anexo(s);

g) autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados.

h) Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição.

i) empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários.

3.4.1. O impedimento de que trata a alínea "a" do item 3.4, supra, será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a

efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.4.2. Durante a vigência do contrato, é vedado ao contratado contratar cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do órgão contratante ou de agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato.

3.4.3. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem as alíneas "g" e "i" poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

3.4.4. O disposto nas alíneas "g" e "i" não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

3.5. A participação de pessoa jurídica em consórcio no presente processo licitatório fica condicionada ao atendimento dos requisitos do art. 15 da Lei 14.133/2021.

3.6. Os profissionais organizados sob a forma de cooperativa poderão participar da presente licitação, desde que:

a) a constituição e o funcionamento da cooperativa observarem as regras estabelecidas na legislação aplicável, em especial a Lei nº 5.764, de 16 de dezembro de 1971, a Lei nº 12.690, de 19 de julho de 2012, e a Lei Complementar nº 130, de 17 de abril de 2009;

b) a cooperativa apresentar demonstrativo de atuação em regime cooperado, com repartição de receitas e despesas entre os cooperados;

c) qualquer cooperado, com igual qualificação, for capaz de executar o objeto contratado.

d) o objeto da licitação referir-se, em se tratando de cooperativas enquadradas na Lei nº 12.690, de 19 de julho de 2012, a serviços especializados constantes do objeto social da cooperativa, a serem executados de forma complementar à sua atuação.

4 – DO MODO DE DISPUTA

4.1. Será adotado o modo de disputa aberto, em que os licitantes apresentarão lances públicos e sucessivos, observando as regras constantes no item **8**.

4.2. A etapa competitiva, de envio de lances na sessão pública, durará **10 (dez) minutos**, e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos **02 (dois) minutos** do período de duração da sessão pública.

4.2.1. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

4.3. Encerrado o prazo do item **4.2**, o sistema encaminhará o aviso de fechamento iminente dos lances e, transcorrido o período de até dez minutos, aleatoriamente determinado, a recepção de lances será automaticamente encerrada.

4.4. Encerrada a recepção dos lances, o sistema ordenará os lances em ordem crescente de vantajosidade.

4.5. Encerrada a sessão pública sem prorrogação automática pelo sistema, o pregoeiro poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances, em prol da consecução do melhor preço, mediante justificativa.

4.6. Na hipótese do sistema eletrônico desconectar para o pregoeiro no decorrer da etapa de envio de lances da sessão pública e permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

4.7. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente decorridas vinte e quatro horas após a comunicação do fato aos participantes, no sítio eletrônico www.garibaldi.rs.gov.br.

4.8. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5 – DO ENVIO DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

5.2. As propostas deverão ser enviados exclusivamente por meio do sistema, até a data e horário estabelecidos no preâmbulo deste edital, observando os itens 5 e 6 deste Edital, e poderão ser retirados ou substituídos até a abertura da sessão pública.

5.2.1. Os documentos de habilitação serão solicitados pelo pregoeiro ao vencedor, concedendo prazo de 02 (duas) horas para que sejam anexados no sistema após a finalização da etapa dos lances e após inserção e ajustes da proposta final.

5.3. O licitante deverá declarar, sendo que a falsidade da declaração sujeitará o licitante às sanções legais:

5.3.1. O cumprimento dos requisitos para a habilitação e a conformidade de sua proposta com as exigências do edital, como condição de participação.

5.3.2. O cumprimento dos requisitos legais para a qualificação como microempresa ou empresa de pequeno porte, microempreendedor individual, produtor rural pessoa física, agricultor familiar ou sociedade cooperativa de consumo, se for o caso, estando apto a usufruir do tratamento favorecido estabelecido nos arts. 42 ao 49 da Lei Complementar nº 123/2006, como condição para aplicação do disposto no item 9, deste edital, mediante apresentação de **declaração de que se enquadra como microempresa ou empresa de pequeno porte, firmada pelo responsável legal e contador ou técnico contábil, com o receptivo CRC, e com data não superior a 60 (sessenta) dias da data da licitação.**

5.3.2.1. Em substituição ao documento supramencionado, poderá ser apresentada Certidão Simplificada, que comprove o enquadramento da Licitante como microempresa ou empresa de pequeno porte, emitida pela Junta Comercial do Estado de sede da Licitante, certificada digitalmente e com data de emissão não superior a 90 (noventa) dias da data da licitação.

5.3.3. Que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

5.3.4. Que não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

OBSERVAÇÃO 01: A empresa que pretender se utilizar dos benefícios previstos nos art. 42 à 45 da Lei Complementar 123, de 14 de dezembro de 2006, e alterações da Lei 147/2014, deverá assinalar em campo próprio do Sistema Pregão Eletrônico Banrisul quando da inclusão das propostas no sistema.

5.4. Eventuais outros documentos complementares à proposta e à habilitação, que venham a ser solicitados pelo pregoeiro, deverão ser encaminhados no prazo máximo de 02 (duas) horas.

5.5. Para fins de habilitação neste pregão, a licitante deverá apresentar os seguintes documentos:

5.5.1. DECLARAÇÕES (MODELO DO ANEXO II):

a) Declaração de Idoneidade;

b) Declaração que atende ao disposto no artigo 7°, inciso XXXIII, da Constituição Federal, conforme o modelo do Decreto Federal n° 4.358/02;

c) Declaração de cumprimento dos requisitos para a habilitação e a conformidade de sua proposta com as exigências do edital, como condição de participação.

d) Declaração de observância do limite de R$ 4.800.000,00 na licitação, limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno

porte.

e) Declaração 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.

f) Declaração que não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

g) Declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social.

h) Declaração da licitante de que não que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, conforme art. 14, IV da Lei nº 14.133/2021.

5.5.2. HABILITAÇÃO JURÍDICA:

a) Ato constitutivo, Estatuto ou contrato social em vigor, devidamente registrado, em caso de sociedades comerciais e, no caso de sociedade por ações, acompanhado de documentos de eleição de seus administradores;

b) Indicação do ato constitutivo, no caso de Sociedades Civis, acompanhada de prova, indicando a diretoria em exercício;

c) Registro Comercial no caso de empresa individual.

5.5.3. REGULARIDADE FISCAL, SOCIAL E TRABALHISTA:

a) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ/MF), com data de emissão de até 12 (doze) meses a data de abertura do certame;

b) Prova de regularidade expedida pela Procuradoria Nacional da Fazenda (**Certidão Conjunta de Débitos relativos a Tributos Federais e à Dívida Ativa da União**).

c) Prova de regularidade com a Fazenda Estadual.

d) Prova de regularidade com a Fazenda Municipal, sendo da sede ou domicílio do Licitante.

e) Prova de regularidade junto ao Fundo de Garantia por tempo de serviço (FGTS) e seguridade social.

f) Certidão Negativa de Débitos Trabalhistas (obtida eletronicamente nos sites do TRT-4 e/ou Regional correspondente do licitante ou TST).

g) Comprovante de inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

5.5.3.1. A microempresa, a empresa de pequeno porte e a cooperativa que possuir restrição em qualquer dos documentos de regularidade fiscal, previstos no subitem **5.5.3.** deste edital, terão sua habilitação condicionada à apresentação de nova documentação, que comprove a sua regularidade em cinco dias úteis, a contar da data em que for declarada vencedora do certame.

5.5.3.2. O benefício de que trata o item anterior não eximirá a microempresa, a empresa de pequeno porte e a cooperativa, da apresentação de todos os documentos, ainda que apresentem alguma restrição.

5.5.3.3. O prazo de que trata o item **5.5.3.1.** poderá ser prorrogado, por uma única vez, por igual período, a critério da Administração, desde que seja requerido pelo interessado, de forma motivada e durante o transcurso do respectivo prazo.

5.5.3.4. A não regularização da documentação, no prazo fixado no item **5.5.3.1**, implicará na decadência do direito à contratação, sem prejuízo das penalidades previstas neste edital, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a licitação.

5.5.4. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

a) Certidão negativa de falência ou concordata expedida pelo distribuidor da sede da pessoa jurídica, em prazo não superior a (90) noventa dias da data da apresentação do documento.

5.5.5. QUALIFICAÇÃO TÉCNICA

a) Comprovação de aptidão para o desempenho de atividade pertinente e compatível em características com o objeto da licitação, por meio da apresentação de 1 (um) ou mais atestados de capacidade técnica, emitidos por pessoa jurídica de direito público ou privado, que comprove(m) sua aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis ou iguais ao objeto presente certame. O(s) atestado(s) deverá(ão) dispor sobre a prestação satisfatória dos referidos serviços, concluídos ou em andamento;

b) Declaração emitida pela fabricante dos equipamentos e softwares comprovando que é um canal autorizado com nível de certificações "Advanced" e que está apta para comercializar as licenças, garantias e suporte técnico dos produtos objetos da contratação;

c) A licitante deve comprovar que possui em seus quadros 01 (um) técnico com certificação em modalidade de "especialista em segurança de redes" ou similar, fornecida pelo fabricante da solução de NGFW;

c.1) A comprovação do vínculo acima referido deverá ser feita da seguinte forma: em se tratando de sócio da empresa, por intermédio da apresentação do contrato social ou no caso de empregado, mediante cópia da Carteira de Trabalho e Previdência Social (CTPS) assinada com data anterior a deste Edital;

5.6. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

a) complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame;

b) atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

5.7. A documentação deverá ser apresentada na sua forma original ou por cópia autenticada, com exceção da documentação eletrônica, que possui autenticação do site oficial.

5.7.1. As empresas licitantes deverão se atentar para apresentação dos documentos correspondentes à proposta financeira e à habilitação, OBRIGATORIAMENTE, em seus RESPECTIVOS CAMPOS E NOS PRAZOS ESPECÍFICOS estabelecidos nas convocações realizadas pelo(a) Agente de Contratação. Ressalta-se que NÃO SERÃO ACEITOS documentos de habilitação anexados conjuntamente com a proposta financeira, inicial ou atualizada, **SOB PENA DE IMEDIATA DESCLASSIFICAÇÃO DA LICITANTE.**

5.8. Para efeito de verificação dos documentos de habilitação, será permitida a sua realização por processo eletrônico de comunicação a distância, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

5.9. Se o envio da documentação ocorrer a partir de sistema informatizado prevendo acesso por meio de chave de identificação e senha do interessado, presume-se a devida segurança quanto à autenticidade e autoria, sendo desnecessário o envio de documentos assinados digitalmente com assinatura eletrônica avançada ou assinatura eletrônica qualificada, nos termos do Decreto Municipal nº 4.765/2023.

5.10. Não serão admitidos atestados de responsabilidade técnica de profissionais que, comprovadamente, tenham dado causa à aplicação das sanções previstas nos incisos III e IV do caput do art. 156 da Lei nº 14.133, de 2021, em decorrência de orientação proposta, de prescrição técnica ou de qualquer ato profissional de sua responsabilidade.

6- DA PROPOSTA DE PREÇO

6.1. A proposta, cujo prazo de validade é fixado pela Administração em **sessenta** (60) dias, deverá ser registrada no sistema eletrônico, observando as diretrizes do **Anexo III**. Também deverá

conter:

a) Razão social da empresa;

b) Preço unitário e total do item, até duas casas após a vírgula, em moeda nacional, devendo estar incluídas quaisquer vantagens, abatimentos, impostos, taxas e contribuições sociais, obrigações trabalhistas, previdenciárias, fiscais e comerciais, que eventualmente incidam sobre a operação ou, ainda, despesas com transporte ou terceiros, as quais correrão por conta da licitante vencedora.

c) Informação de marca/modelo ofertada que deverá ser observada na entrega, **se for o caso**.

d) Informação do fabricante do produto, **se for o caso.**

e) Descrição do objeto, contendo as informações de acordo com a especificação do Termo de Referência;

f) Indicação do prazo de garantia do produto, de acordo com a Lei nº 8.078, de 11 de setembro de 1990, **se for o caso.**

6.2. Serão desclassificadas as propostas que se apresentarem em desconformidade com este edital, bem como, com preços superestimados ou inexequíveis, ou superiores ao estimado pela Administração.

6.3. Todas as especificações do objeto contidas na proposta vinculam o licitante.

6.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto, exceto em caso de erro grosseiro, questão que será avaliada pelo pregoeiro.

6.5. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

6.6. As empresas licitantes deverão se atentar para apresentação dos documentos correspondentes à proposta financeira e à habilitação, OBRIGATORIAMENTE, em seus RESPECTIVOS CAMPOS E NOS PRAZOS ESPECÍFICOS estabelecidos nas convocações realizadas pelo(a) Agente de Contratação. Ressalta-se que NÃO SERÃO ACEITOS documentos de habilitação anexados conjuntamente com a proposta financeira, inicial ou atualizada, **SOB PENA DE IMEDIATA DESCLASSIFICAÇÃO DA LICITANTE.**

7 – DA ABERTURA DA SESSÃO PÚBLICA

7.1. No dia e hora indicados no preâmbulo, o pregoeiro abrirá a sessão pública, mediante a utilização de sua chave e senha.

7.2. O licitante poderá participar da sessão pública na internet, mediante a utilização de sua chave de acesso e senha, e deverá acompanhar o andamento do certame e as operações realizadas no sistema eletrônico durante toda a sessão pública do pregão, ficando responsável pela perda de negócios diante da inobservância de mensagens emitidas pelo sistema ou de sua desconexão, conforme item **3.3.** deste Edital.

7.3. A comunicação entre o pregoeiro e os licitantes ocorrerá mediante troca de mensagens em campo próprio do sistema eletrônico.

7.4. Iniciada a sessão, as propostas de preços contendo a descrição do objeto e do valor estarão disponíveis na *internet*.

7.5. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

8– DA CLASSIFICAÇÃO INICIAL DAS PROPOSTAS E FORMULAÇÃO DE LANCES

8.1. O pregoeiro verificará as propostas apresentadas e desclassificará fundamentadamente aquelas que não estejam em conformidade com os requisitos estabelecidos no edital.

8.2. Será desclassificada a proposta que:

a) Contiver vícios insanáveis;
b) Não obedecer às especificações técnicas contidas no Termo de Referência;
c) Apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;
d) Não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;
e) Apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

8.2.1. Na hipótese de a proposta vencedora não for aceitável ou o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao edital.

8.2.2. No caso de bens e serviços em geral, a Administração considerará indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração, facultando ao Pregoeiro diligenciar, conforme item 8.3.

8.2.3. No caso de serviços de engenharia, serão consideradas inexequíveis as propostas cujos valores forem inferiores a 75% (setenta e cinco por cento) do valor orçado pela Administração, independentemente do regime de execução.

8.3. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

8.4. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação.

8.4.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

8.4.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

8.5. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

8.5.1. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

8.6. Quaisquer inserções na proposta que visem modificar, extinguir ou criar direitos, sem previsão no edital, serão tidas como inexistentes, aproveitando-se a proposta no que não for conflitante com o instrumento convocatório.

8.7. As propostas classificadas serão ordenadas pelo sistema e o pregoeiro dará início à fase competitiva, oportunidade em que os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico.

8.8. Somente poderão participar da fase competitiva os autores das propostas classificadas.

8.9. Os licitantes poderão oferecer lances sucessivos e serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do seu autor, observando o horário fixado para duração da etapa competitiva, e as seguintes regras:

8.9.1. O licitante será imediatamente informado do recebimento do lance e do valor consignado no registro.

8.9.2. O licitante somente poderá oferecer valor inferior ao último lance por ele ofertado e registrado pelo sistema.

8.9.3. Não serão aceitos dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro.

8.9.4. O intervalo mínimo de diferença de valores entre os lances será de 01 (um) minuto, que incidirá tanto em relação aos lances intermediários, quanto em relação do lance que cobrir a melhor oferta.

8.10. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

8.11. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta, será determinado previamente via sistema.

8.12. Na licitação para registro de preços não será admitida a cotação de quantitativo inferior ao máximo previsto no edital, sob pena de desclassificação.

8.13. Somente serão considerados válidos os lances dos licitantes que forem inseridos na "sala de disputa", não sendo considerados outros meios, tais como chat do sistema, e-mail, etc.

9 - DO CRITÉRIO DE DESEMPATE

9.1. Encerrada etapa de envio de lances, será apurada a ocorrência de empate, nos termos dos arts. 44 e 45 da Lei Complementar nº 123/2006, sendo assegurada, como critério do desempate, preferência de contratação para as beneficiárias da referida Lei.

9.1.1. Entende-se como empate aquelas situações em que as propostas apresentadas pela microempresa e pela empresa de pequeno porte, bem como pela cooperativa, sejam iguais ou superiores em até 5% (cinco por cento) à proposta de menor valor.

9.1.2. A situação de empate somente será verificada depois de ultrapassada a fase da proposta e encerrados os lances.

9.2. Ocorrendo o empate, na forma do item anterior, proceder-se-á da seguinte forma:

a) a microempresa, a empresa de pequeno porte ou a cooperativa, detentora da proposta de menor valor, poderá apresentar, no prazo de 05 (cinco) minutos, nova proposta, inferior àquela considerada, até então, de menor preço, situação em que será declarada vencedora do certame.

b) Se a microempresa, a empresa de pequeno porte ou a cooperativa, convocada na forma da alínea anterior, não apresentar nova proposta, inferior à de menor preço, será facultada, pela ordem de classificação, às demais microempresas, empresas de pequeno porte ou cooperativas remanescentes, que se enquadrarem na hipótese do item **9.1.1** deste edital, a apresentação de nova proposta, no prazo e na forma prevista na alínea "a" deste item.

c) Se houver duas ou mais microempresas e/ou empresas de pequeno porte e/ou cooperativas com propostas iguais, será realizado sorteio para estabelecer a ordem e serão convocadas para a apresentação de nova proposta, na forma das alíneas anteriores.

9.3. Se não houver licitante que atenda ao item 9.2. e seus subitens, serão utilizados os seguintes critérios de desempate, nesta ordem:

a) Disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

b) Avaliação do desempenho contratual prévio dos licitantes, para a qual serão ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações decorrentes de outras contratações;

c) Desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme Decreto nº 4.172, de 1º de setembro de 2023;

d) Desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

9.4. Em igualdade de condições, se não houver desempate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

a) Empresas estabelecidas no território do Estado do Rio Grande do Sul;

b) Empresas brasileiras;

c) Empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

d) empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de

dezembro de 2009.

10 – NEGOCIAÇÃO E JULGAMENTO

10.1. Encerrada a etapa de envio de lances da sessão pública, inclusive com a realização do desempate, se for o caso, o pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste edital.

10.2. A negociação será encerrada após transcorridos 15 (quinze) minutos da sua abertura, exceto se as partes entrarem em acordo antes desse período.

10.3. Encerrada a etapa de negociação, será examinada a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação valor de referência da Administração.

10.4. Não serão consideradas, para julgamento das propostas, vantagens não previstas no edital.

10.5. O licitante vencedor terá o prazo de 2 (duas) horas, prorrogável por decisão do pregoeiro, contado da solicitação do pregoeiro no sistema, para envio da proposta e, se necessário, dos documentos complementares, adequada ao último lance ofertado após a negociação de que trata o caput deste artigo.

10.6. Será permitido o registro de mais de um fornecedor, desde que a cotação seja em preço igual ao do licitante vencedor, assegurada a preferência de contratação de acordo com a ordem de classificação.

10.7. O licitante vencedor terá o prazo de 2 (duas) horas, contado da solicitação do pregoeiro no sistema, para envio da proposta e, dos documentos complementares, adequada ao último lance ofertado após a negociação de que trata o caput deste artigo.

10.7.1. A critério do pregoeiro, o prazo supramencionado, poderá ser prorrogado, uma única vez, em até 120 (cento e vinte) minutos;

11 – DA VERIFICAÇÃO DA HABILITAÇÃO

11.1. Encerrada a etapa de negociação, caso entenda necessário, o pregoeiro poderá verificar se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União; e

c) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União.

11.2. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

11.3. Os documentos de habilitação, de que trata o item 5.5, serão examinados pelo pregoeiro, que verificará a autenticidade das certidões junto aos sítios eletrônicos oficiais de órgãos e entidades emissores.

11.3.1. As certidões apresentadas na habilitação, que tenham sido expedidas em meio eletrônico, serão tidas como originais após terem a autenticidade de seus dados e certificação digital conferidos pela Administração, dispensando nova apresentação, exceto se vencido o prazo de validade.

11.4. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

11.5. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital.

11.6. Na análise dos documentos de habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante despacho fundamentado registrado em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

11.7. A beneficiária da Lei Complementar nº 123/2006 que possua alguma restrição na comprovação de regularidade fiscal e/ ou trabalhista, terá sua habilitação condicionada ao envio de nova documentação, que comprove a sua regularidade, em 5 (cinco) dias úteis, prazo que poderá ser prorrogado uma única vez, por igual período, a critério da Administração, desde que seja requerido pelo interessado, de forma motivada e durante o transcurso do respectivo prazo.

11.8. Caso a licitação dependa da verificação da Planilha de Custos, a sessão será suspensa para análise pela secretaria competente para, após, ser adjudicada.

11.8.1. Nesse caso, a empresa vencedora, declarada na fase dos lances, deverá apresentar ao pregoeiro, em até 48 horas contados da realização do certame, uma planilha de custos detalhada, conforme modelo em anexo, com todos os valores unitários e total. A planilha será encaminhada para a Secretaria competente para análise dos valores e o certame ficará suspenso para posterior adjudicação.

12– DOS RECURSOS ADMINISTRATIVOS E IMPUGNAÇÕES

12.1. Declarado o vencedor, ou proclamado o resultado sem que haja um vencedor, os licitantes poderão manifestar justificadamente a intenção de interposição de recurso, em campo próprio do sistema, durante o prazo de 10 (dez) minutos, encerrado este prazo automaticamente pelo sistema, sob pena de decadência do direito de recurso.

12.2. Havendo a manifestação motivada do interesse em recorrer, será concedido o prazo de 3 (três) dias úteis para a interposição das razões do recurso, também via sistema, ficando os demais licitantes desde logo intimados para apresentar contrarrazões em igual número de dias, que começarão a correr do término do prazo do recorrente.

12.2.1. O recurso deverá versar sobre:

a) Ato que defira ou indefira pedido de pré-qualificação de interessado ou de inscrição em registro cadastral, sua alteração ou cancelamento;

b) Julgamento das propostas;

c) Ato de habilitação ou inabilitação de licitante;

d) Anulação ou revogação da licitação.

12.2.2. Quanto ao recurso apresentado em virtude do disposto nas alíneas "b" e "c" do item **12.2.1** do presente Edital, serão observadas as seguintes disposições:

a) a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão, e o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

b) A apreciação dar-se-á em fase única.

12.3. O recurso e as contrarrazões serão dirigidos à autoridade que tiver editado o ato ou proferido a decisão recorrida, que, se não reconsiderar o ato ou a decisão no prazo de 3 (três) dias úteis, encaminhará o recurso com a sua motivação à autoridade superior, a qual deverá proferir sua decisão no prazo máximo de 10 (dez) dias úteis, contado do recebimento dos autos.

12.4. O acolhimento do recurso implicará invalidação apenas de ato insuscetível de aproveitamento.

12.5. O recurso interposto dará efeito suspensivo ao ato ou à decisão recorrida, até que sobrevenha decisão final da autoridade competente.

12.6. A impugnação ao edital de licitação deve ser protocolada em até 3 (três) dias úteis antes da data de abertura do certame. A resposta à impugnação ou ao pedido de esclarecimento será divulgada em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

12.6.1. A impugnação deverá ser encaminhada ao e-mail licitacoes@garibaldi.rs.gov.br, o qual servirá como protocolo oficial.

12.6.2. As respostas aos pedidos de esclarecimentos e às impugnações serão encaminhadas para o endereço eletrônico da impugnante e divulgadas no sítio eletrônico da Administração.

12.7. Os recursos, impugnações e contrarrazões interpostos fora do prazo não serão conhecidos.

12.8. A licitante poderá encaminhar pedido de reconsideração, no prazo de 3 (três) dias úteis, contado da data de intimação, relativamente a ato do qual não caiba recurso hierárquico.

13– DO ENCERRAMENTO DA CONTRATAÇÃO

13.1. Encerradas as fases de julgamento e habilitação, e exauridos os recursos administrativos, o processo licitatório será encaminhado à autoridade superior, que poderá:

a) Determinar o retorno dos autos para saneamento de irregularidades;

b) Revogar a licitação por motivo de conveniência e oportunidade;

c) Proceder à anulação da licitação, de ofício ou mediante provocação de terceiros, sempre que presente ilegalidade insanável;

d) Adjudicar o objeto e homologar a licitação.

14 – DAS CONDIÇÕES DE CONTRATAÇÃO

14.1. O licitante vencedor receberá o termo de contrato ou o instrumento equivalente, preferencialmente via digital, para assinatura imediata, devendo devolver o documento no prazo máximo de 07 dias úteis do recebimento, podendo este prazo ser prorrogado 1 (uma) vez, por igual período, mediante solicitação da parte, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

14.2. Expirado o prazo sem assinatura, será facultado à Administração, convocar os licitantes remanescentes, na ordem de classificação, para a celebração do contrato nas condições propostas pelo licitante vencedor.

14.3. Decorrido o prazo de validade da proposta indicado no item 14.1 deste Edital, sem convocação para a contratação, ficarão os licitantes liberados dos compromissos assumidos.

14.4. Na hipótese de nenhum dos licitantes aceitar a contratação, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

a) Convocar os licitantes remanescentes para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário;

b) Adjudicar e celebrar o contrato nas condições ofertadas pelos licitantes remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

14.5. A recusa injustificada do adjudicatário em assinar o contrato ou o instrumento equivalente no prazo estabelecido pela Administração caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas, previstas neste edital, e à imediata perda da garantia de proposta em favor do órgão licitante.

14.6. A vencedora deverá observar durante a execução do contrato as normas técnicas aplicáveis ao serviço, bem como as normas de segurança do trabalho.

14.7. A vencedora deverá executar os serviços observando fielmente o Termo de Referência, inclusive em relação à qualidade dos materiais e ao cronograma de execução, e os termos da sua proposta.

14.8. A vencedora deverá manter, durante toda a execução contratual, todas as condições de habilitação e qualificação exigidas na licitação, inclusive quanto às contribuições para o FGTS e INSS relativa aos empregados utilizados na prestação do serviço, devendo apresentar mensalmente à Administração os comprovantes de pagamentos dos encargos trabalhistas e previdenciários.

14.9. Antes de formalizar ou prorrogar o prazo de vigência do contrato, a Administração verificará a regularidade fiscal do contratado, consultar o Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e o Cadastro Nacional de Empresas Punidas (Cnep), emitir as certidões negativas de inidoneidade, de impedimento e de débitos trabalhistas e juntá-las ao respectivo processo.

14.10. A gestão do presente contrato ou instrumento equivalente será feita pelo servidor

DANIEL DECONTI, matrícula 5324, tendo como obrigação:

a) conferir a existência de empenho prévio à realização da despesa;

b) acompanhar a publicação tempestiva do extrato do contrato;

c) conferir a existência de designação de fiscal para o contrato celebrado pela Administração;

d) controlar os limites de acréscimo e de supressão nas obras, serviços ou compras, inclusive em atas de registro de preços, em conformidade com a legislação;

e) adotar as providências para a confecção tempestiva dos termos aditivos, quando for o caso, atendidas as formalidades previstas na legislação.

f) receber ou formular os pedidos de repactuação e de reequilíbrio econômico-financeiro, encaminhando-os para os órgãos competentes realizarem a análise correspondente, submetendo-os à autoridade;

g) deliberar sobre o pedido de substituição do responsável técnico, desde que este detenha experiência e qualificação equivalente ou superior ao substituído, a ser verificada de acordo com as regras do processo que deu origem à contratação;

h) examinar, periodicamente, a atualização e a adequação da documentação do contratado em relação às obrigações trabalhistas, previdenciárias e fiscais, notificando-o em caso de irregularidade, dando ciência à autoridade, sugerindo a aplicação de sanção e a rescisão contratual se persistir o descumprimento, observados ampla defesa e o contraditório;

i) manifestar-se sobre eventual pedido de subcontratação;

j) executar outras atividades determinadas pelo superior hierárquico.

14.4. O responsável pela fiscalização do contrato será o servidor MARCELO DE BORBA, matrícula 5.110, que terá como obrigação:

a) conhecer os termos do processo de contratação e as condições do contrato, em especial os prazos, os cronogramas, as obrigações das partes, os casos de rescisão, a existência de cláusula de modificação do preço, se for o caso, e as hipóteses de aditamento;

b) acompanhar e fiscalizar a execução da obra, do serviço ou do fornecimento de bens, em estrita observância ao edital e ao contrato;

c) juntar documentos, registrar telefonemas, fazer anotações, redigir atas de reunião, anexar correspondências, inclusive as eletrônicas, e quaisquer documentos relativos à execução do contrato, no processo de fiscalização;

d) registrar todas as ocorrências durante a execução do contrato, solicitando ao Departamento Jurídico a notificação por escrito do contratado, que deverá conter determinação para saneamento das faltas ou defeitos observados em prazo a ser estipulado de acordo com o caso concreto;

e) fazer cumprir fielmente as obrigações avençadas, relatando por escrito e sugerindo à autoridade superior a aplicação das sanções, na forma do edital e do contrato, no caso de inadimplência, garantindo ao contratado o direito de defesa;

f) conferir a conclusão das etapas e o cumprimento das condições de pagamento;

g) dar recebimento provisório das obras, serviços e compras mediante termo circunstanciado;

h) dar recebimento definitivo das obras, serviços e compras mediante termo circunstanciado, se houver previsão expressa na portaria de designação; e

i) executar outras atividades determinadas pelo superior hierárquico.

14.11. A extinção do contrato poderá ser:

a) determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;

b) consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

c) determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

14.13. DO REAJUSTE/REEQUILÍBRIO/REPACTUAÇÃO

14.13.1. No vencimento do contrato os preços poderão ser reajustados, se for o caso, até o

índice do IPCA, com data-base vinculada à data do orçamento estimado, respeitado o interregno de um ano para concessão.

14.13.2. A contratada, em função da dinâmica do mercado, poderá solicitar a atualização dos preços vigentes, mediante solicitação à Administração Municipal, acompanhada de documentos que comprovem a procedência do pedido.

14.13.3. A atualização não poderá ultrapassar o preço praticado no mercado e deverá manter a diferença percentual apurada entre o preço originalmente constante da proposta e o preço de mercado vigente à época.

14.13.4. O pedido de reequilíbrio somente será analisado pela Administração Pública após a inequívoca comprovação da ocorrência do fato gerador que ensejou o alegado desequilíbrio no fluxo financeiro da Contratada.

14.13.5. Considerando-se que o equilíbrio exigido na relação contratual envolve uma contraposição entre encargos e vantagens, não serão concedidos reequilíbrios que ensejam impacto irrisório ao Contratante.

14.13.6. A base de cálculo do reajuste anual será o valor da proposta financeira apresentada, com o acréscimo, se houver, de eventuais correções inflacionárias decorrentes do decurso de prazo contratual, sendo descontada a porcentagem dos reequilíbrios concedidos durante a contratação.

14.13.7. Poderá haver repactuação sempre que houver regime de dedicação exclusiva de mão de obra ou predominância de mão de obra, mediante demonstração analítica da variação dos custos.

14.13.8. O pedido de repactuação deve solicitado pela CONTRATADA e observado o interregno mínimo de 01 (um) ano contado da data da apresentação da proposta ou da data da última repactuação, competindo à CONTRATADA justificar e comprovar a variação dos custos, apresentando memória de cálculo e planilhas apropriadas para análise e posterior aprovação da CONTRATANTE;

14.13.9. A repactuação poderá ser dividida em tantas parcelas quantas forem necessárias, em respeito ao princípio da anualidade do reajustamento dos preços da contratação, podendo ser realizada em momentos distintos para discutir a variação de custos que tenham sua anualidade resultante em datas diferenciadas, tais como os custos decorrentes da mão de obra e os custos decorrentes dos insumos necessários à execução do serviço.

14.13.10. O interregno mínimo de 01 (um) ano para a primeira repactuação será contado:

14.13.10.1. Para os custos relativos à mão de obra, vinculados à data-base da categoria profissional: a partir dos efeitos financeiros do acordo, dissídio ou convenção coletiva de trabalho, vigente à época da apresentação da proposta, relativo a cada categoria profissional abrangida pelo contrato;

14.13.10.2. Para os insumos discriminados na Planilha de Custos e Formação de Preços que estejam diretamente vinculados ao valor de preço público (tarifa): do último reajuste aprovado por autoridade governamental ou realizado por determinação legal ou normativa;

14.13.10.3. Para os demais custos, sujeitos à variação de preços do mercado (insumos não decorrentes da mão de obra): a partir da data limite para apresentação das propostas constantes do Edital.

14.13.11. Nas repactuações subsequentes à primeira, o interregno de um ano será computado da última repactuação correspondente à mesma parcela objeto de nova solicitação. Entende-se como última repactuação, a data em que iniciados seus efeitos financeiros, independentemente daquela em que celebrada ou apostilada.

14.13.12. O prazo para a CONTRATADA solicitar a repactuação encerra-se na data da prorrogação contratual subsequente ao novo acordo, dissídio ou convenção coletiva que fixar os novos custos de mão de obra da categoria profissional abrangida pelo contrato, ou na data do encerramento da vigência do contrato, caso não haja prorrogação.

14.13.13. Caso a CONTRATADA não solicite a repactuação tempestivamente, dentro do prazo acima fixado, ocorrerá a preclusão do direito à repactuação.

14.13.14. Nessas condições, se a vigência do contrato tiver sido prorrogada, nova repactuação só poderá ser pleiteada após o decurso de novo interregno mínimo de 01 (um) ano, contado:

14.13.14.1. Da vigência do acordo, dissídio ou convenção coletiva anterior, em relação aos custos decorrentes de mão de obra;

14.13.14.2. Do último reajuste aprovado por autoridade governamental ou realizado por determinação legal ou normativa, para os insumos discriminados na Planilha de Custos e Formação de Preços que estejam diretamente vinculados ao valor de preço público (tarifa); e

14.13.14.3. Do dia em que se completou um ou mais anos da apresentação da proposta, em relação aos custos sujeitos à variação de preços do mercado;

14.13.15. Caso, na data da prorrogação contratual, ainda não tenha sido celebrado o novo acordo, dissídio ou convenção coletiva da categoria, ou ainda não tenha sido possível à CONTRATANTE ou à CONTRATADA proceder aos cálculos devidos, deverá ser inserida cláusula no termo aditivo de prorrogação para resguardar o direito futuro à repactuação, a ser exercido tão logo se disponha dos valores reajustados, sob pena de preclusão.

14.13.16. A repactuação de preços será formalizada por apostilamento ou termo aditivo.

OBSERVAÇÃO: o prazo para resposta ao pedido de repactuação de preços será, preferencialmente de 1 (um) mês, contado da data do fornecimento da documentação.

15– DOS PRAZOS E DO FORNECIMENTO

15.1. O prazo de vigência da contratação será de até 12 (doze) meses, a contar da assinatura do contrato, podendo ser prorrogado sucessivamente por meio de Termo Aditivo, até atingir o limite máximo de 10 anos de vigência, nos limites do artigo 107 da Lei 14.133/2021, a critério da Secretaria Contratante.

15.1.1. A data base para contagem dos prazos contratuais será definida a partir da homologação da licitação e estará registrada no contrato firmado entre as partes.

15.2. A aceitação do objeto somente será efetivada após ter sido o mesmo considerado satisfatório, pela fiscalização do(s) contrato(s), ficando a empresa fornecedora obrigada a substituí-lo, em parte ou integralmente, em tempo hábil, sempre que ocorrerem falhas.

16 – DO PAGAMENTO

16.1. Os pagamentos serão efetuados mensalmente até o 30º (trigésimo) dia, contado a partir do recebimento da respectiva nota fiscal no setor de empenhos, desde que haja a devida comprovação da prestação dos serviços, atestada pelo fiscal, conforme Calendário de Pagamentos a Fornecedores, correndo a despesa na:

ÓRGÃO 13 – SECRETARIA MUNICIPAL DE INOVAÇÃO E EMPREENDEDORISMO
UNIDADE 1 - SECRETARIA MUNICIPAL DE INOVAÇÃO E EMPREENDEDORISMO
23.691.0094.2084 - MANUTENÇÃO DOS SERVIÇOS DA SMIE
3.3.9.04 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – (1340)
3.3.9.04.01.30 - COMUNICAÇÃO DE DADOS – (134013)

16.2. A forma de pagamento será por meio de crédito em conta bancária, devendo a contratada informar banco, agência, operação e número da conta bancária em nome da contratada, ou através de boleto de cobrança bancária.

a) Quando a cobrança ocorrer por boleto, o mesmo somente poderá ser emitido com código de barra padrão FEBRABAN com vencimento apresentação.

16.3. Caso o objeto do certame seja passível de retenção de imposto, conforme IN/RFB 1234/12 e IN/RFB 971/09, a contratada ficará sujeita à aplicação desta.

16.4. A nota fiscal/fatura emitida pelo fornecedor deverá conter, em local de fácil visualização, a indicação do nº do Pregão e da Ordem de Fornecimento, a fim de se acelerar o trâmite de recebimento do material e posterior liberação do documento fiscal para pagamento.

16.5. Na hipótese de existência de erros na nota fiscal de cobrança e/ou outra circunstância que impeça a liquidação da despesa, o pagamento será interrompido e ficará pendente até que a CONTRATADA adote as medidas saneadoras, voltando a correr na sua íntegra após a CONTRATADA ter solucionado o problema, seguindo a legislação vigente quanto à ordem cronológica de pagamentos do CONTRATANTE.

16.6. Em caso de atraso no pagamento por parte e por motivação da contratante, o valor devido será atualizado monetariamente com base no IPCA (IBGE), considerando-se a variação no período compreendido entre a data do vencimento e a data do efetivo pagamento.

17 – DAS OBRIGAÇÕES

17.1. Das obrigações da CONTRATADA:

a) prestar os serviços de acordo com as especificações do contrato e as solicitações da Administração;

b) disponibilizar veículos em perfeitas condições de uso, conservação, limpeza, segurança e regularidade perante os órgãos competentes;

c) disponibilizar motoristas devidamente habilitados e qualificados para a condução dos veículos;

d) manter frota e estrutura operacional suficientes para atender às demandas simultâneas da Administração;

e) arcar com todas as despesas decorrentes da execução do contrato, incluindo combustível, manutenção preventiva e corretiva, tributos, seguros, encargos trabalhistas, previdenciários e demais custos;

f) responder por quaisquer danos causados ao Município, aos usuários ou a terceiros em decorrência da execução dos serviços;

g) manter, durante toda a vigência contratual, as condições de habilitação e qualificação exigidas na licitação;

h) comunicar imediatamente à Administração qualquer ocorrência que possa comprometer a execução dos serviços;

17.2. DO MUNICÍPIO:

a) Prestar informações e os esclarecimentos atinentes ao objeto, que venham a ser solicitados pela licitante;

b) Efetuar o pagamento nas condições e preços pactuados;

c) Fiscalizar a execução do objeto do contrato por meio de servidor designado;

18 – DAS SANÇÕES ADMINISTRATIVAS

18.1. O licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações:

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.
m) Não assinar a ata de registro de preços, **se for o caso**.

18.2. Serão aplicadas ao responsável pelas infrações administrativas previstas no item 18.1 deste edital as seguintes sanções:

a) advertência, quando der causa à inexecução parcial do contrato, e não se justificar a imposição de penalidade mais grave.

b) multa, a ser calculada na forma do edital ou do contrato, não podendo ser inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato, que será aplicada ao responsável por qualquer das infrações administrativas previstas no item 18.1.

c) impedimento de licitar e contratar, pelo prazo máximo de 3 (três) anos, quando do cometimento das infrações administrativas previstas nas alíneas "b", "c", "d", "e", "f" e "g" do item 18.1, quando não se justificar a imposição de penalidade mais grave.

d) declaração de inidoneidade para licitar ou contratar, quando do cometimento das infrações administrativas previstas nas alíneas "h", "i", "j", "l" e m do item 18.1, bem como pelas infrações administrativas previstas nas alíneas "b", "c", "d", "e", "f" e "g", do item 18.1 que justifiquem a imposição de penalidade mais grave que a sanção referida na alínea c do item 18.2, que 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.

e) multa de 2% sobre o valor total do contrato, além das penalidades já utilizadas e previstas na legislação, em caso de descumprimento de normas trabalhistas.

18.2.1. As sanções previstas nas alíneas "a", "c" e "d" do item 18.2 do presente Edital poderão ser aplicadas cumulativamente com a prevista na alínea "b" do mesmo item.

18.2. 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 o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

18.3. A sanção estabelecida na alínea "d" do item 18.2 será precedida de análise jurídica e observará e será aplicada pela autoridade máxima municipal;

18.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

18.5. A aplicação das sanções previstas no item 18.2 deste Edital não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

18.6. Na aplicação da sanção prevista no item 18.2, alínea "b", do presente edital, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

18.7. Para aplicação das sanções previstas nas alíneas "c" e "d" do item 18.2 do presente Edital dependerá de instauração de processo de responsabilização, a ser conduzido por comissão composta de no mínimo 3 (três) servidores, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o contratado para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

18.7.1. Na hipótese de deferimento de pedido de produção de novas provas ou de juntada de provas julgadas indispensáveis pela comissão, o licitante ou o contratado poderá apresentar alegações finais no prazo de 15 (quinze) dias úteis, contado da data da intimação.

18.7.2. Serão indeferidas pela comissão, mediante decisão fundamentada, provas ilícitas, impertinentes, desnecessárias, protelatórias ou intempestivas.

18.8. A personalidade jurídica poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos nesta Lei ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

18.9. Sobrevindo aplicação de nova penalidade no curso do período das sanções previstas nas alíneas "c" e "d" do item 18.2 deste edital, será somado ao período remanescente o fixado na nova decisão condenatória, reiniciando-se os efeitos das sanções.

18.9.1. Na soma envolvendo sanções previstas nas alíneas "c" e "d" do item 18.2, observar-se-á o prazo máximo de 6 (seis) anos em que o condenado poderá ficar proibido de licitar ou contratar com a Administração Pública Municipal.

18.9.2. Para o cálculo da soma contam-se as condenações em meses, desprezando-se os dias, respeitando-se o limite máximo previsto no item 18.10.1 deste edital, orientado pelo termo inicial da primeira condenação.

18.10. É admitida a reabilitação do licitante ou contratado perante a própria autoridade que aplicou a penalidade, exigidos, cumulativamente:

a) Reparação integral do dano causado à Administração Pública;

b) Pagamento da multa;

c) transcurso do prazo mínimo de 1 (um) ano da aplicação da penalidade, no caso de impedimento de licitar e contratar, ou de 3 (três) anos da aplicação da penalidade, no caso de declaração de inidoneidade;

d) Cumprimento das condições de reabilitação definidas no ato punitivo;

e) Análise jurídica prévia, com posicionamento conclusivo quanto ao cumprimento dos requisitos definidos neste artigo.

18.10.1. A reabilitação alcança quaisquer penas aplicadas em decisão definitiva, assegurando ao licitante e ao contratado o sigilo dos registros sobre o seu processo e condenação.

19 - DAS DISPOSIÇÕES GERAIS

19.1. Quaisquer informações ou dúvidas de ordem técnica, bem como aquelas decorrentes de interpretação do edital, deverão ser solicitadas ao Setor de Licitações, sito na Rua Júlio de Castilhos, nº 254, pelo telefone (54) 3462-8228 ou através do e-mail licitacoes@garibaldi.rs.gov.br, no horário compreendido entre as 8h às 11h30min e das 13h30min às 17h, preferencialmente, com antecedência mínima de 03 (três) dias da data marcada para abertura do certame.

19.2. Ocorrendo decretação de feriado ou qualquer fato superveniente que impeça a realização de ato do certame na data marcada, a data constante deste edital será transferida, automaticamente, para o primeiro dia útil ou de expediente normal subsequente ao ora fixado.

19.3. Para agilização dos trabalhos, solicita-se que as licitantes façam constar na documentação o seu endereço, e-mail e o número de telefone.

19.4. Todos os documentos exigidos no presente instrumento convocatório deverão ser apresentados em original ou por qualquer processo de cópia autenticada por tabelião ou servidor do Município, ainda, publicação em órgão da imprensa oficial. Os documentos extraídos de sistemas informatizados (Internet) ficarão sujeitos à verificação da autenticidade de seus dados e de sua validade, pela Administração.

19.5. A proponente que vier a ser contratada ficará obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, por conveniência da Administração, dentro do limite permitido pelo artigo 125 da Lei nº 14.133/2021, sobre o valor inicial atualizado do contratado.

19.6. Após a apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo pregoeiro.

19.7. A apresentação de proposta significa a aceitação dos termos desta licitação e vincula as partes nos termos do diploma jurídico que a rege.

19.8. Administração tem a prerrogativa de fiscalizar o cumprimento satisfatório do objeto da presente licitação, por meio de agente designado para tal função, conforme o disposto na Lei nº 14.133/2021.

19.9. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

19.10. Este edital está à disposição dos interessados no horário das 8 horas às 11 horas e 30 minutos e das 13h30min às 17h, na Prefeitura Municipal de Garibaldi, na Rua Júlio de Castilhos, nº 254, telefone (54) 3462-8228, ou, no site www.garibaldi.rs.gov.br.

19.11. São anexos deste Edital:

ANEXO I - MODELO DE CREDENCIAMENTO
ANEXO II - MODELO DE DECLARAÇÕES
ANEXO III – MODELO DE PROPOSTA DE PREÇOS
ANEXO IV – MODELO DE MINUTA DE CONTRATO
ANEXO V – TERMO DE REFERÊNCIA

19.12. Fica eleito, de comum acordo entre as partes, o Foro da Comarca de Garibaldi, para dirimir quaisquer litígios oriundos da licitação e do contrato decorrente, com expressa renúncia a outro qualquer, por mais privilegiado que seja.

Garibaldi, 23 de setembro de 2026.

DANIEL DECONTI
Secretário Municipal de Inovação e Empreendedorismo

Assinado digitalmente por:
JESSICA PIMENTEL DA SILVA
***.423.700-**
24/09/2026 08:53:31 -03:00

JÉSSICA PIMENTEL DA SILVA
Departamento de Compras e Licitações

Com exceção do "objeto", sobre o qual está Assessoria Jurídica não possui conhecimento técnico para se manifestar, este edital se encontra examinado e aprovado por esta Assessoria.

RENATA AGOSTINI - OAB/RS 78.649
Assessora Jurídica
Procuradoria Geral do Município

A N E X O I – MODELO DE CREDENCIAMENTO
PREGÃO Nº ___/2026

CREDENCIAMENTO

CREDENCIADO

Nome: _____

Nacionalidade: _____Estado Civil: _____

Endereço: _____Profissão: _____

Nº da Identidade: _____CPF: _____

E-mail:_____

EMPRESA CREDENCIADORA

Nome: _____

Endereço: _____

CNPJ/MF: _____Inscrição Estadual:_____

Através deste instrumento de credenciamento, a empresa acima descrita, nomeia o CREDENCIADO acima qualificado, para seu representante na licitação, modalidade Pregão Eletrônico nº __, promovida pelo Município de Garibaldi, conferindo-lhe todos os poderes necessários para a prática dos atos licitatórios previstos na Lei Federal nº 14.133 de 1º de abril de 2021 e Decreto nº 4.765/2023, podendo o mesmo tudo assinar e requerer, em especial, ofertar lances, protestar, ingressar com manifestação de recursos, receber notificações, abdicar de direitos e assinar contratos e aditivos oriundos daquele certame licitatório.

_____de ____de _____.

_____
NOME DO RESPONSÁVEL EMPRESA CREDENCIADORA

A N E X O II – MODELO DE DECLARAÇÃO CONJUNTA
PREGÃO Nº ___/2026

DADOS DA EMPRESA

RAZÃO SOCIAL: _____

CNPJ/MF/Nº_____INSCRIÇÃO ESTADUAL: _____

ENDEREÇO: _____

Na qualidade de representante legal da empresa acima descrita, declaro sob as penas da lei e para fins da licitação Modalidade Pregão Eletrônico nº ____, que a Empresa por mim apresentada:

( ) não está suspensa temporariamente da participação em licitações, nem impedida de contratar com o Poder Público e, da mesma forma não está na situação de empresa inidônea para licitar ou contratar com o Poder Público.
( ) não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.
( ) cumpre os requisitos para a habilitação e a conformidade de sua proposta com as exigências do edital, como condição de participação.
( ) está em observância ao limite de R$ 4.800.000,00 na licitação, limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.
( ) apresenta proposta econômica que compreende 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.
( ) não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;
( ) cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, nos limites previstos no art. 93 da Lei nº 8.213, de 24 de julho de 1991.
( ) não mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, conforme art. 14, IV da Lei nº 14.133/2021.

Ressalva CASO EMPREGUE MENOR: emprega menor, a partir de quatorze anos, na condição de aprendiz ( ).

LOCAL: _____, _____de _____de _____.
ASSINATURA:
NOME:

A N E X O III – MODELO DE PROPOSTA DE PREÇOS
PREGÃO Nº _____/2026

PROPOSTA DE PREÇOS

Empresa_____
Endereço_____
CNPJ/MF/Nº_____ Insc.Estadual:_____
Fone/Fax_____ e-mail:_____
Data da abertura: **08 DE OUTUBRO DE 2026** Horário**: 08 horas e 30 minutos**
Conta Bancária para depósito para pagamento em caso de ser vencedor:
Banco_____ Nº Agência_____ Nº Conta nº_____
Declaro-me de pleno acordo com os termos e condições do Edital modalidade **Pregão Eletrônico nº _____/2026**, apresentando a seguinte proposta financeira, para fornecimento do seguinte serviço:

1.1. A presente licitação tem por objeto a contratação de empresa especializada para a locação de solução de Firewall de Próxima Geração (Next Generation Firewall – NGFW), por meio de appliance em hardware dedicado, incluindo o fornecimento dos equipamentos, licenciamento integral de todas as funcionalidades, instalação, configuração, migração da solução atualmente em operação, suporte técnico especializado, garantia, manutenção corretiva, atualização de firmware e de assinaturas de segurança, bem como todos os demais serviços necessários ao pleno funcionamento da solução durante toda a vigência contratual, nos termos das tabelas abaixo, conforme condições e exigências estabelecidas neste edital.

LOTE ÚNICO					
ITEM	**OBJETO**	**QTDE**	**UN**	**VALOR UNITÁRIO**	**VALOR TOTAL**
01	SERVIÇOS DE LOCAÇÃO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL – NGFW), COMPREENDENDO O FORNECIMENTO DE APPLIANCE EM HARDWARE DEDICADO, LICENCIAMENTO COMPLETO DE TODAS AS FUNCIONALIDADES DE SEGURANÇA, SUPORTE TÉCNICO, GARANTIA, ATUALIZAÇÕES DE FIRMWARE, ASSINATURAS DE SEGURANÇA (IPS, ANTIVÍRUS, ANTIMALWARE, FILTRO DE CONTEÚDO WEB, CONTROLE DE APLICAÇÕES E WEB APPLICATION FIREWALL – WAF), ALÉM DO SERVIÇO DE LOGGING ANALYTICS PARA ARMAZENAMENTO, PROCESSAMENTO E ANÁLISE DOS REGISTROS (LOGS) GERADOS PELO EQUIPAMENTO. 10GB/DIA	12	UN		
02	IMPLEMENTAÇÃO	01	UN		
				VALOR TOTAL DO LOTE R$	

1.2. A solução de NGFW a ser fornecida através de "*appliance*" com capacidade de Inspeção profunda de pacotes (DPI), análise detalhada do tráfego para identificar ameaças ocultas, prevenção contra intrusões (IPS/IDS) e bloqueio proativo de tentativas de exploração de vulnerabilidades, além de oferecer a possibilidade de auditoria dos acessos realizados através da emissão e gestão de relatórios especializados.

1.3. A solução deverá atuar como principal mecanismo de proteção do perímetro da rede

corporativa e da rede interna da Administração Municipal, realizando inspeção, monitoramento e controle de todo o tráfego de dados entre a rede interna e a Internet, bem como entre segmentos internos da infraestrutura tecnológica, prevenindo acessos não autorizados, ataques cibernéticos e demais ameaças que possamcomprometer a disponibilidade, integridade e confidencialidade das informações.

1.4. A solução deverá contemplar, no mínimo, funcionalidades de Firewall Stateful, inspeção profunda de pacotes (Deep Packet Inspection – DPI), controle de aplicações por camada 7 (Layer 7), identificação de usuários, administração de largura de banda (QoS), VPN IPsec, Sistema de Prevenção e Detecção de Intrusão (IPS/IDS), proteção contra vírus, malwares e demais códigos maliciosos, filtro de conteúdo web, inspeção de tráfego criptografado (SSL Inspection), proteção de aplicações web (Web Application Firewall – WAF), geração de relatórios especializados e mecanismos avançados de auditoria dos acessos realizados.

1.5. A solução deverá incluir serviço de Logging Analytics, responsável pelo armazenamento, indexação, pesquisa e análise dos registros de eventos (logs) gerados pelo equipamento, permitindo a rastreabilidade das ações realizadas na rede, emissão de relatórios gerenciais, auditoria de eventos de segurança e apoio às atividades de monitoramento e resposta a incidentes. A capacidade mínima contratada deverá ser de 10 GB de ingestão de logs por dia, atendendo ao consumo atual da infraestrutura municipal e prevendo margem para o crescimento da demanda durante a vigência contratual.

1.6. Também deverão integrar a contratação todas as licenças necessárias ao funcionamento integral da solução, incluindo atualizações de firmware, assinaturas de antivírus, antimalware, IPS, filtro de conteúdo web, controle de aplicações, Web Application Firewall (WAF) e demais componentes de segurança, sem qualquer custo adicional para a Administração durante todo o período da locação.

1.7. A contratada será responsável pela instalação física e lógica da solução, configuração dos equipamentos, migração das políticas de segurança atualmente existentes, integração com o ambiente de auditoria e gerenciamento de logs já implantado pelo Município, realização de testes de funcionamento, homologação da solução, treinamento operacional da equipe técnica e prestação de suporte técnico especializado durante toda a vigência do contrato.

1.8. A solução deverá ser compatível com instalação em rack padrão de 19 polegadas, conforme norma EIA-310, ocupando no máximo 1U de altura, e deverá garantir níveis adequados de desempenho para suportar o volume de tráfego da rede municipal, assegurando a continuidade dos serviços públicos digitais e permitindo futuras expansões da infraestrutura tecnológica sem necessidade de substituição prematura da solução contratada.

1.9. Por se tratar de uma solução integrada de hardware, software, licenciamento e serviços especializados, todos os componentes deverão ser fornecidos por uma única contratada, garantindo total compatibilidade entre os equipamentos, funcionalidades e serviços prestados, bem como maior eficiência na gestão contratual, na manutenção da solução e na responsabilização técnica durante toda a execução do contrato.

1.10. Fornecimento de solução de NGFW com as seguintes características:

1.10.1. CARACTERÍSTICAS DO HARDWARE:

• O equipamento deve ser compatível com instalação em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45 mm);

• Dispor de pelo menos duas fontes de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz cada;

• Possuir painel ou led indicador on/off e devices de rede;

• Possuir throughput de no mínimo 26 Gbps para tráfego UDP independente do tamanho dos pacotes;

• Suportar no mínimo 2.900.000 (dois milhões e novecentas mil) conexões simultâneas;

• Suportar no mínimo 130.000 (cento e trinta mil) novas conexões por segundo;

• Possuir throughput mínimo de 5 Gbps para tráfego IPS/IDS;

• Possuir throughput mínimo de 30Gbps para tráfego VPN IPSEC;

• Possuir throughput mínimo de 3 Gbps para tráfego NGFW (habilitadas as funcionalidades

de Firewall, IPS e Controle de Aplicativo);

• Possuir pelo menos 16 (dezesseis) interfaces de rede Gigabit Ethernet 10/100/1000, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

• Possuir no mínimo 4 lans 10GBE SFP+;

• Possuir no mínimo 8 lans 1GBE SFP;

• Possuir no mínimo 1 (uma) porta console de conexão para acesso à interface de comando CLI específica para esta finalidade;

• Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos.

1.10.2. ESPECIFICAÇÃO GERAL DO SOFTWARE NGFW:

1.10.2.1. FUNÇÕES BÁSICAS

• Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;
• Agentless VPN, VPN ipsec (Client-to-site e Site-to-site);
• Controle de Aplicações;
• Proxy Web e Filtro de Conteúdo Web (URL Filtering);
• Detecção e prevenção de intrusos – IPS;
• Qualidade de serviço – QoS;
• Anti-Malware;
• SD-WAN;
• Cluster.

1.10.2.2. CARACTERÍSTICAS GERAIS

• Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui *stateful firewall* 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, IPS, prevenção contra ameaças de vírus, malwares, filtro de URL, inspeção de tráfego criptografado e proteção de firewall de aplicação Web.

• Interface em português e inglês;

• O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

• Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução;

• A solução deverá ser em hardware dedicado tipo *appliance* com sistema operacional customizado para garantir segurança e melhor desempenho;

• Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;

• Não deve ser necessária a instalação de qualquer software no dispositivo cliente para realizar o acesso ou a administração dos recursos do equipamento, bem como adição e utilização de servidores e/ou appliances.

1.10.2.3. FUNCIONALIDADES DO FIREWALL

• Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;

• Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

• Deve possuir ferramentas para realizar backups de forma remota, por SSH, FTP, NFS ou próprio do fabricante. Deve também permitir backup em Pen-drive. A solução deve permitir o agendamento diário ou semanal do backup;

• Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.

• Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica;

• As cópias de segurança devem ser salvas criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

• Deve permitir habilitar ou desabilitar o registro de log por política de firewall.

• Possuir controle de acesso à internet por endereço IP de origem e destino;
• Possuir controle de acesso à internet por sub-rede;
• Possuir suporte a tags de VLAN (802.1q);
• Suportar agregação de links, segundo padrão IEEE 802.3ad;
• Possuir ferramenta de diagnóstico do tipo pcap;
• Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;
• Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
• Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.
• Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
• Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;
• Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
• Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;
• Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
• Deverá suportar aplicações multimídia como: H.323, SIP;
• Possuir tecnologia de firewall do tipo Stateful;
• Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo/passivo e ativo/ativo;
• Permitir o funcionamento em modo transparente tipo "bridge";
• Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;
• Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);
• Deverá suportar forwarding de multicast;
• Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP e UDP;
• Permitir o agrupamento de serviços;
• Permitir o filtro de pacotes sem a utilização de NAT;
• Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
• Possuir mecanismo de anti-spoofing;
• Permitir criação de regras definidas pelo usuário;
• Permitir o serviço de autenticação para HTTP e FTP;
• Possuir a funcionalidade de balanceamento e contingência de links;
• 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.
• Deve dar suporte e ter licenciada a virtualização de firewall, permitindo a criação de, no mínimo, 5 (cinco) firewalls virtuais (contextos ou domínios virtuais), onde cada um possa assumir logicamente em modo de NGFW e ainda possibilitar o uso de interfaces de redes, endereçamentos, políticas e roteamentos distintos.
• Todas as funcionalidades devem estar disponíveis em todos os contextos, não havendo limitações de uso quando sendo apenas o firewall base ou seus contextos virtualizados.
• Deve permitir a criação de administradores independentes, para cada um dos firewalls virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que possam ser administrados por equipes distintas.

1.10.2.4. IDENTIFICAÇÃO DO USUÁRIO

• Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;
• 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;

• 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;

• A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

• 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;

• A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;

1.10.2.5. FUNCIONALIDADE DE REDE VIRTUAL PRIVADA (VPN)

• VPN baseada em appliance;
• Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
• Suporte a certificados PKI X.509 para construção de vpns;
• Possuir suporte a vpns ipsec site-to-site:
• Criptografia, 3DES, AES128, AES256, AES-GCM-128
• Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
• Algoritmo Internet Key Exchange (IKE) versões I e II;
• AES 128 e 256 (Advanced Encryption Standard);
• Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14;
• Deve permitir a arquitetura de vpn hub and spoke;
• Suporte a vpns ipsec client-to-site;

• Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);

• Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicosentre múltiplos dispositivos (spokes) com um gateway centralizador (hub).

1.10.2.6. FUNCIONALIDADE DO SISTEMA DE DETECÇÃO DE INTRUSÃO - IPS/IDS

• A Detecção de Intrusão deverá ser baseada em appliance;
• Possuir no mínimo 7.000 assinaturas ou regras de IPS/IDS;
• O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
• Possuir tecnologia de detecção baseada em assinatura;

• Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo bypass;

• O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;

• Possuir opção para administrar as listas de Blacklist, Whitelist e Quarentena com suporte a endereços ipv6;

• 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;

• Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (dos) do tipo Flood, Prot Scan e Sweep;

• Mecanismos de detecção/proteção de ataques;
• Reconhecimento de padrões;
• Análise de protocolos;
• Detecção de anomalias;
• Detecção de ataques de RPC (Remote procedure call);
• Proteção contra ataques de Windows ou netbios;

• Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

• Proteção contra ataques DNS (Domain Name System);
• Proteção contra ataques a FTP, SSH , Telnet e rlogin;
• Proteção contra ataques de ICMP (Internet Control Message Protocol);

• Alertas via correio eletrônico;
• 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;
• Capacidade de resposta ativa a ataques;
• Terminação de sessões via TCP resets;
• Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
• O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
• Possuir filtros de ataques por anomalias;
• Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
• Permitir filtros de anomalias de protocolos;
• Suportar reconhecimento de ataques de dos, reconnaissance, exploits e evasion;
• Suportar verificação de ataque nas camadas de aplicação;

1.10.2.7. FUNCIONALIDADE DE QoS

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

1.10.2.8. FUNCIONALIDADE DO ANTIVÍRUS

• Possuir funções de Antivírus, Anti-spyware;
• Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;
• Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);
• Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

1.10.2.9. FUNCIONALIDADE DO PROXY E FILTRO DE CONTEÚDO

• Possuir solução de filtro de conteúdo web integrado a solução de segurança;
• Possuir pelo menos 85 categorias para classificação de sites web;
• Possuir base mínima contendo, 1 milhão de sites internet web já registrados e classificados;
• 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;
• Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
• Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;
• Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;
• Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;
• Possibilitar a integração com servidores de cache WEB externos;

• Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®;

• 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;

• Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

• Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;

• 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;

• Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;

• Permitir a criação de listas personalizadas de urls permitidas – lista branca e bloqueadas – lista negra;

• Deverá permitir o bloqueio de urls inválidas cujo campo CN do certificado SSL não contém um domínio válido;

• Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;

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

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

• Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;

• Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;

• Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e urls originadas de Spam;

• Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;

• Deverá permitir configurar a porta do Proxy Explícito.

1.10.2.10. FUNCIONALIDADE DO CONTROLE DE APLICAÇÕES

• As funcionalidades abaixo devem ser baseadas em Appliance:

• Reconhecer pelo menos 3.000 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/Video ou Audio, proxy ou tunelamento, mensagens instantâneas ou colaboração, compartilhamento de arquivos/storage, backup, mail;

• Reconhecer pelo menos as seguintes aplicações: 4Shared, Active Directory/SMB, Citrix ICA, DHCP Protocol, 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;

• 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, Vídeo Streaming/Play, Upload);

• Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

• 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, port hopping e túnel através de tráfego SSL encriptado;

• Atualizar a base de assinaturas de aplicações automaticamente;

• Reconhecer aplicações em ipv6;

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

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

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

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

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

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

• Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;

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

1.10.2.11. SISTEMA DE PROTEÇÃO ACANÇADA CONTRA AMEAÇAS - ATP

• Possuir sistema de proteção avançada contra ameaças (ATP) nativo;

• 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;

• 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;

• A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;

• Deve permitir a identificação de aplicativos e ameaças independente das portas e protocolos;

• 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;

• Deve permitir a atualização automática das assinaturas por meio de agendamento diário;

• Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, ataques P2P, trojans, worms, malwares para mobile, blacklist, vulnerabilidades conhecidas;

• Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;

• Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, ataques P2P, trojans, worms, malwares para mobile, blacklist, vulnerabilidades conhecidas;

• Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de voip tais como: Hotline, SIP, Skype;

• 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;

• Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: bittorrent, Gnutella, Napster e de Storages, tais como: Dropbox, Google Drive, Mega e onedrive;

• Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

• Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;

• Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as

"ameaças detectadas" e as "ameaças bloqueadas";

• Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "aplicativos detectados" e os "aplicativos bloqueados";

• Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";

• 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.

1.10.2.12. SD-WAN (GERÊNCIA DE WAN)

• 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;

• Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;

• Permitir utilizar VPN ipsec para interligar unidades remotas;

• Possuir recurso de "persistência de link" para impedir a queda de conexões em aplicações que não suportam o load balance de link;

• 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;

• Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos relacionado ao recurso SD-WAN;

• Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações: Consumo de banda; Perda de pacotes; Jitter; Latência.

1.10.2.13. ALTA DISPONIBILIDADE

• Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Passivo ou Ativo/Ativo, com as implementações de Fail Over;

• 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;

• O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat.

1.10.2.14. REDUNDÂNCIA PARA MÚLTIPLOS ISPs (Provedores)

• A solução proposta deve suportar o balanceamento de carga e redundância para pelo menos 2 (dois) links de Internet;

• A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação;

• A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP;

• A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway;

• A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego ipv4 e ipv6.

1.10.3. FERRAMENTA DE GESTÃO DE RELATÓRIOS

1.10.3.1. CARACTERÍSTICA DA FERRAMENTA

• Deve ser do tipo appliance virtual (VM)

• Possuir capacidade de recebimento de logs de pelo menos 10 mil dispositivos

• Possuir a capacidade de receber pelo menos 9 Gbits de logs diários

• Deverá ser compatível com ambiente VMware ESXi 6.5 e superior

• Deverá ser compatível com ambiente Microsoft Hyper-V 2016, 2019 e 2022

• Deverá ser compatível com ambiente Citrix XenServer 8.2 e superior e Open Source Xen 4.2.5

• Deverá ser compatível com ambiente KVM

• Deverá ser compatível com ambiente Nutanix AHV

- Deverá ser compatível com ambiente Amazon Web Services (AWS)
- Deverá ser compatível com ambiente Microsoft Azure.
- Deverá ser compatível com o ambiente Google Cloud (GCP)
- Deverá ser compatível com o ambiente Oracle Cloud Infrastructure (OCI)
- Deverá ser compatível com o ambiente Alibaba Cloud (AliCloud)
- Não deve possuir limite na quantidade de múltiplas vCPU
- Não deve possuir limite para suporte a expansão de memória RAM

1.10.3.2. REQUISITOS MÍNIMOS DE FUNCIONALIDADE

- Suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções
- Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento.
- Permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento.
- Suportar SNMP versão 2 e 3
- Permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.
- Permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.
- Permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH
- Possuir autenticação de usuários para acesso à plataforma via LDAP
- Possuir autenticação de usuários para acesso à plataforma via Radius
- Possuir autenticação de usuários para acesso à plataforma via TACACS +
- Possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico
- Possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas.
- Possuir geração de relatórios de tráfego em tempo real, em formato de gráfico
- Possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.
- Possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.
- Possuir visualização da quantidade de logs enviados de cada dispositivo monitorado
- Possuir mecanismos de apagamento automático para logs antigos.
- Permitir importação e exportação de relatórios
- Deve ter a capacidade de criar relatórios no formato HTML
- Deve ter a capacidade de criar relatórios em formato PDF
- Deve ter a capacidade de criar relatórios no formato XML
- Deve ter a capacidade de criar relatórios no formato CSV
- Deve permitir exportar os logs no formato CSV
- Deve gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.
- Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.
- A solução deve ter relatórios predefinidos
- Deve poder enviar automaticamente os logs para um servidor FTP externo para a solução
- A duplicação de relatórios existentes deve ser possível para edição posterior.
- Ter a capacidade de personalizar a capa dos relatórios obtidos.
- Permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.
- Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados.
- Ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas
- Deve ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo

real.

- Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo.
- Ter a capacidade de gerar e enviar relatórios periódicos automaticamente.
- Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.
- Permitir o envio por e-mail relatórios automaticamente.
- Deve permitir que o relatório seja enviado por email ao destinatário específico.
- Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.
- É necessário exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.
- Deve permitir o uso de filtros nos relatórios.
- Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.
- Permitir especificar o idioma dos relatórios criados
- Gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.
- Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.
- Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.
- Possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros.
- Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.
- Importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.
- Deve ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.
- Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.
- Deve ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.
- Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos
- Deve permitir visualizar em tempo real os logs recebidos.
- Deve permitir o encaminhamento de log no formato syslog.
- Deve permitir o encaminhamento de log no formato CEF (Common Event Format).
- Deve disponibilizar painel de operações SOC composto por widgets configuráveis, permitindo o monitoramento de eventos de segurança, ameaças, usuários, aplicações, tráfego de rede, VPN, redes sem fio, endpoints, indicadores operacionais da plataforma e demais informações provenientes dos dispositivos integrados, conforme as funcionalidades suportadas pela solução
- Suportar a configuração Master / Slave de alta disponibilidade na camada 3
- Gerar alertas de eventos a partir de logs recebidos
- Permitir a criação de incidentes a partir de alertas de eventos para o terminal
- Permitir a integração ao sistema de tickets do ServiceNow
- Incluir serviço Indicadores de Comprometimento (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredicto (classificação geral da ameaça), o número de ameaças detectadas.
- Deve permitir o suporte a logs na nuvem pública do Amazon S3
- Deve permitir o suporte a logs na nuvem pública do Microsoft Azure
- Permitir o suporte aos registros de nuvem pública do Gooogle Cloud

- Suportar o padrão SAML para autenticação do usuário administrador
- Relatórios de Firewall
- Deve ter um relatório de conformidade com o PCI DSS
- Possuir um relatório de uso do aplicativo SaaS
- Possuir um relatório de prevenção de perda de dados (DLP)
- Possuir um relatório de VPN
- Possuir um relatório IPS (Intruder Prevention System)
- Possuir um relatório de reputação do cliente
- Possuir um relatório de análise de segurança do usuário
- Possuir um relatório de análise de ameaças cibernéticas
- Possuir um breve relatório resumido diário de eventos e incidentes de segurança
- Possuir um relatório de tráfego DNS
- Possuir um relatório de tráfego de e-mail
- Possuir um relatório dos 10 principais aplicativos usados na rede
- Possuir um relatório dos 10 principais sites usados na rede
- Possuir um relatório de uso de mídia social

1.11. ACORDO DE NÍVEL DE SERVIÇO - SLA

1.11.1. A LICITANTE deverá providenciar os atendimentos dentro das regras estabelecidas nesta seção:

- suporte técnico prestado em horário comercial, de segunda a sexta-feira com os seguintes prazos:

a) o atendimento virtual (remoto) de até 30 minutos após a abertura do chamado;

b) o atendimento presencial (quando necessário) em até 04 horas úteis após a abertura do chamado;

1.12. SUPORTE TÉCNICO

1.12.1. A licitante deverá prover suporte técnico necessário para garantir o perfeito funcionamento da solução descrita neste termo, bem como zelar pela resolução de possíveis incidentes no nível de serviço exigido, visando a não interrupção dos serviços contratados.

1.12.2. A empresa licitante deverá fornecer no mínimo dois canais de suporte ao cliente, sendo ao menos um canal por via digital, sendo aceito sistema web, formulário em site, atendimento via Whatsapp ou outros similares, desde que, possuam a capacidade de registrar e emitir comprovante de abertura de chamado;

1.12.3. Toda solicitação de suporte emitida pela Prefeitura de Garibaldi deverá ser registrada e controlada através da Central de Suporte da licitante contendo, minimamente, os dados de data e horário da abertura do chamado, identificação do solicitante e do técnico que receberá o chamado para iniciar o atendimento.

1.12.4. Os custos de Suporte Técnico deverão estar incluídos e distribuídos nos preços unitários.

1.12.5. Serão consideradas como Suporte Técnico todas as atividades empreendidas pela licitante necessárias para assegurar o funcionamento dos equipamentos, com o objetivo de possibilitar a continuidade dos serviços instalados e de garantir a alta disponibilidade objetiva.

1.12.6. O Suporte Técnico deverá ser acionável e realizado de segunda a sexta, no horário das 08:00 às 11:30 horas e das 13:30 às 17:00 horas, compreendendo:

a) manutenção corretiva: série de procedimentos destinados a reparar e a corrigir os componentes dos equipamentos e serviços, sem ônus à Prefeitura de Garibaldi, mantendo seu pleno estado de funcionamento, removendo definitivamente os defeitos eventualmente apresentados;

b) manutenção adaptativa: série de procedimentos destinados a adequar os itens de configuração em razão de alterações no ambiente tecnológico que suporta os equipamentos e serviços devendo a licitante informar à Prefeitura de Garibaldi a necessidade de atualização de qualquer software relativo à solução de NGFW;

c) A sede/filial da licitante deverá estar localizada a no máximo 130 quilômetros do Centro Administrativo da prefeitura, viabilizando o prazo de atendimento presencial;

1.13. IMPLANTAÇÃO

1.13.1. A solução de NGFW atualmente existente no município é do fabricante FORTINET, utilizando o hardware "Fortigate 80F" com firmware na versão 7.4.12, o sistema de auditoria e gestão de relatórios está configurado em ambiente virtual, utilizando a plataforma Hyper-V da Microsoft;

1.13.2. O processo de implantação tem por objetivo a inserção do hardware e software na infraestrutura da PREFEITURA de forma que o resultado final seja uma solução de NGFW com as mesmas características de organização interna (regras de firewall, conexões com AD, interfaceamento, VLANS, etc.) da solução atual;

1.13.3. A PREFEITURA designará um profissional responsável para acompanhamento e fornecimento de todas as informações pertinentes à implantação;

1.13.4. Todas as atividades relativas à implantação deverão acontecer em dias úteis (SEGUNDA-SEXTA) no intervalo das 08:00 – 17:00hs, remotamente ou presencialmente, de acordo com a necessidade;

1.13.5. A LICITANTE deverá fornecer um plano de implantação contendo minimamente as etapas e prazos para ser atingidos até a conclusão da implantação e início da prestação do serviço. Este plano deverá ser submetido ao Departamento de T.I do município para avaliação e posterior liberação para início dos trabalhos de implantação;

1.13.5.1. Em caso da solução de NGFW ser do mesmo fabricante da solução atual do município, a LICITANTE poderá substituir o plano de implantação por acesso prévio à nova solução para avaliar a migração direta das configurações através da cópia/restauração do arquivo de configuração;

1.13.6. A solução a ser adquirida deverá ser configurada de maneira que não seja necessário aquisição de novo hardware ou software para o seu pleno funcionamento;

1.13.7. A solução a ser adquirida deverá ser configurada de maneira que não seja necessário alterações estruturais no formato de organização da floresta/domínio do Active Directory pertencente ao município de Garibaldi;

1.13.8. A LICITANTE deverá fornecer credenciais com permissões suficientes para que os técnicos do Município de Garibaldi consigam fazer o gerenciamento COMPLETO da solução, incluindo todas as áreas abrangentes ao funcionamento e layout de conexão, criação e alteração de usuários administradores;

1.14. O prazo de início será a partir da assinatura do contrato, momento a partir do qual a contratada estará autorizada a realizar a instalação, configuração e ativação dos serviços contratados.

1.15. Deverão ser fornecidos todo hardware e licenças para uso e atualização de todos os componentes de software, vacinas de antivírus/malwares, assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período vigente da locação;

1.16. Para os itens que representem bens materiais, a LICITANTE deverá fornecer produtos novos, sem uso anterior. Por cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento;

1.17. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-ofsale, 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;

1.18. Toda solução fornecida deverá estar coberta por danos causados por eventos de força maior, com origem elétrica ou do meio ambiente, devendo ser imediatamente substituído sem custos adicionais ao CONTRATANTE;

1.19. O prazo de entrega e ativação da solução é de 30 (trinta) dias corridos contados da data de emissão da ordem de compra;

1.20. A solução deverá ser entregue e configurada na Prefeitura Municipal de Garibaldi, localizada na Rua Júlio de Castilhos, 254, Bairro Centro, Garibaldi/RS.

1.21. O prazo de vigência da contratação será de até 12 (doze) meses, a contar da assinatura do contrato, podendo ser prorrogado sucessivamente por meio de Termo Aditivo, até atingir o limite máximo de 10 anos de vigência, nos limites do artigo 107 da Lei 14.133/2021, a critério da Secretaria Contratante.

1.22. Caso haja algum serviço em desacordo com as especificações constantes no Termo de Referência e na proposta ou que seja de péssima qualidade, deverão ser reparados no prazo de 15 (quinze) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades. Neste caso, a nota fiscal será retida até que seja regularizada a pendência, sendo autorizado o pagamento após a liberação da pessoa responsável.

O município de Garibaldi é optante de assinaturas digitais e deve atender as especificações contidas no Decreto Municipal nº 4.765/2023.

Caso a empresa seja optante de assinatura digital, favor informar o responsável legal, CPF e-mail para envio da documentação:
Nome: _____ CPF: _____E-mail: _____

Validade da Proposta: 60 dias
Local: _____, ____de _____de _____.
Assinatura: _____
Nome do Responsável: _____

A N E X O IV - MINUTA DE CONTRATO
PREGÃO Nº ___/2026

O presente termo trata-se de uma minuta podendo ocorrer alterações quando de sua formalização, desde que não afetem cláusulas pétreas do edital, cabendo ao contratante sua conferência por ocasião da assinatura.

Contrato celebrado entre o **MUNICÍPIO DE GARIBALDI/RS,** sito na Rua Júlio de Castilhos, 254, inscrito no CNPJ nº 88.594.999/0001-95, através da Secretaria Municipal de Inovação e Empreendedorismo, representada neste ato pelo Secretário DANIEL DECONTI, nomeado pela portaria nº xxx/xxxx e portador da matrícula funcional nº xxxx, doravante denominada CONTRATANTE e, a **empresa XXXXXXXXXXXXXXXXXXXXXX,** com sede na Rua ....., nº ....., Bairro ....., no município de ....., RS, CEP: ....., inscrita no CNPJ sob nº ....., neste ato devidamente representada por sua responsável legal XXXXXXXXXXXXXXXXX, conforme atos constitutivos da empresa, a seguir denominada CONTRATADA, em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, tem entre si justo e acordado celebrar o presente Contrato de Prestação de Serviços, oriundo do Processo de Licitação por Pregão Eletrônico nº 098/2026 e pelas condições que estipulam a seguir.

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente instrumento tem por objeto a contratação de empresa especializada para a locação de solução de Firewall de Próxima Geração (Next Generation Firewall – NGFW), por meio de appliance em hardware dedicado, incluindo o fornecimento dos equipamentos, licenciamento integral de todas as funcionalidades, instalação, configuração, migração da solução atualmente em operação, suporte técnico especializado, garantia, manutenção corretiva, atualização de firmware e de assinaturas de segurança, bem como todos os demais serviços necessários ao pleno funcionamento da solução durante toda a vigência contratual, nos termos das tabelas abaixo, conforme condições e exigências estabelecidas no edital de Pregão Eletrônico nº 098/2026.

LOTE ÚNICO			
ITEM	**OBJETO**	**QTDE**	**UN**
01	SERVIÇOS DE LOCAÇÃO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL – NGFW), COMPREENDENDO O FORNECIMENTO DE APPLIANCE EM HARDWARE DEDICADO, LICENCIAMENTO COMPLETO DE TODAS AS FUNCIONALIDADES DE SEGURANÇA, SUPORTE TÉCNICO, GARANTIA, ATUALIZAÇÕES DE FIRMWARE, ASSINATURAS DE SEGURANÇA (IPS, ANTIVÍRUS, ANTIMALWARE, FILTRO DE CONTEÚDO WEB, CONTROLE DE APLICAÇÕES E WEB APPLICATION FIREWALL – WAF), ALÉM DO SERVIÇO DE LOGGING ANALYTICS PARA ARMAZENAMENTO, PROCESSAMENTO E ANÁLISE DOS REGISTROS (LOGS) GERADOS PELO EQUIPAMENTO. 10GB/DIA	12	UN
02	IMPLEMENTAÇÃO	01	UN

1.2. A solução de NGFW a ser fornecida através de "*appliance*" com capacidade de Inspeção profunda de pacotes (DPI), análise detalhada do tráfego para identificar ameaças ocultas, prevenção contra intrusões (IPS/IDS) e bloqueio proativo de tentativas de exploração de vulnerabilidades, além de oferecer a possibilidade de auditoria dos acessos realizados através da emissão e gestão de relatórios especializados.

1.3. A solução deverá atuar como principal mecanismo de proteção do perímetro da rede corporativa e da rede interna da Administração Municipal, realizando inspeção, monitoramento e controle de todo o tráfego de dados entre a rede interna e a Internet, bem como entre segmentos internos da infraestrutura tecnológica, prevenindo acessos não autorizados, ataques cibernéticos e demais ameaças que possamcomprometer a disponibilidade, integridade e confidencialidade das informações.

1.4. A solução deverá contemplar, no mínimo, funcionalidades de Firewall Stateful, inspeção profunda de pacotes (Deep Packet Inspection – DPI), controle de aplicações por camada 7 (Layer 7), identificação de usuários, administração de largura de banda (QoS), VPN IPsec, Sistema de Prevenção e

Detecção de Intrusão (IPS/IDS), proteção contra vírus, malwares e demais códigos maliciosos, filtro de conteúdo web, inspeção de tráfego criptografado (SSL Inspection), proteção de aplicações web (Web Application Firewall – WAF), geração de relatórios especializados e mecanismos avançados de auditoria dos acessos realizados.

1.5. A solução deverá incluir serviço de Logging Analytics, responsável pelo armazenamento, indexação, pesquisa e análise dos registros de eventos (logs) gerados pelo equipamento, permitindo a rastreabilidade das ações realizadas na rede, emissão de relatórios gerenciais, auditoria de eventos de segurança e apoio às atividades de monitoramento e resposta a incidentes. A capacidade mínima contratada deverá ser de 10 GB de ingestão de logs por dia, atendendo ao consumo atual da infraestrutura municipal e prevendo margem para o crescimento da demanda durante a vigência contratual.

1.6. Também deverão integrar a contratação todas as licenças necessárias ao funcionamento integral da solução, incluindo atualizações de firmware, assinaturas de antivírus, antimalware, IPS, filtro de conteúdo web, controle de aplicações, Web Application Firewall (WAF) e demais componentes de segurança, sem qualquer custo adicional para a Administração durante todo o período da locação.

1.7. A contratada será responsável pela instalação física e lógica da solução, configuração dos equipamentos, migração das políticas de segurança atualmente existentes, integração com o ambiente de auditoria e gerenciamento de logs já implantado pelo Município, realização de testes de funcionamento, homologação da solução, treinamento operacional da equipe técnica e prestação de suporte técnico especializado durante toda a vigência do contrato.

1.8. A solução deverá ser compatível com instalação em rack padrão de 19 polegadas, conforme norma EIA-310, ocupando no máximo 1U de altura, e deverá garantir níveis adequados de desempenho para suportar o volume de tráfego da rede municipal, assegurando a continuidade dos serviços públicos digitais e permitindo futuras expansões da infraestrutura tecnológica sem necessidade de substituição prematura da solução contratada.

1.9. Por se tratar de uma solução integrada de hardware, software, licenciamento e serviços especializados, todos os componentes deverão ser fornecidos por uma única contratada, garantindo total compatibilidade entre os equipamentos, funcionalidades e serviços prestados, bem como maior eficiência na gestão contratual, na manutenção da solução e na responsabilização técnica durante toda a execução do contrato.

1.10. Fornecimento de solução de NGFW com as seguintes características:

1.10.1. CARACTERÍSTICAS DO HARDWARE:

• O equipamento deve ser compatível com instalação em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45 mm);

• Dispor de pelo menos duas fontes de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz cada;

• Possuir painel ou led indicador on/off e devices de rede;

• Possuir throughput de no mínimo 26 Gbps para tráfego UDP independente do tamanho dos pacotes;

• Suportar no mínimo 2.900.000 (dois milhões e novecentas mil) conexões simultâneas;

• Suportar no mínimo 130.000 (cento e trinta mil) novas conexões por segundo;

• Possuir throughput mínimo de 5 Gbps para tráfego IPS/IDS;

• Possuir throughput mínimo de 30Gbps para tráfego VPN IPSEC;

• Possuir throughput mínimo de 3 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

• Possuir pelo menos 16 (dezesseis) interfaces de rede Gigabit Ethernet 10/100/1000, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

• Possuir no mínimo 4 lans 10GBE SFP+;

• Possuir no mínimo 8 lans 1GBE SFP;

• Possuir no mínimo 1 (uma) porta console de conexão para acesso à interface de comando CLI específica para esta finalidade;

• Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos.

1.10.2. ESPECIFICAÇÃO GERAL DO SOFTWARE NGFW:

1.10.2.1. FUNÇÕES BÁSICAS

• Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;

• Agentless VPN, VPN ipsec (Client-to-site e Site-to-site);

• Controle de Aplicações;
• Proxy Web e Filtro de Conteúdo Web (URL Filtering);
• Detecção e prevenção de intrusos – IPS;
• Qualidade de serviço – QoS;
• Anti-Malware;
• SD-WAN;
• Cluster.

1.10.2.2. CARACTERÍSTICAS GERAIS

• Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui *stateful firewall* 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, IPS, prevenção contra ameaças de vírus, malwares, filtro de URL, inspeção de tráfego criptografado e proteção de firewall de aplicação Web.

• Interface em português e inglês;

• O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

• Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução;

• A solução deverá ser em hardware dedicado tipo *appliance* com sistema operacional customizado para garantir segurança e melhor desempenho;

• Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;

• Não deve ser necessária a instalação de qualquer software no dispositivo cliente para realizar o acesso ou a administração dos recursos do equipamento, bem como adição e utilização de servidores e/ou appliances.

1.10.2.3. FUNCIONALIDADES DO FIREWALL

• Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;

• Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

• Deve possuir ferramentas para realizar backups de forma remota, por SSH, FTP, NFS ou próprio do fabricante. Deve também permitir backup em Pen-drive. A solução deve permitir o agendamento diário ou semanal do backup;

• Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.

• Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica;

• As cópias de segurança devem ser salvas criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

• Deve permitir habilitar ou desabilitar o registro de log por política de firewall.
• Possuir controle de acesso à internet por endereço IP de origem e destino;
• Possuir controle de acesso à internet por sub-rede;
• Possuir suporte a tags de VLAN (802.1q);
• Suportar agregação de links, segundo padrão IEEE 802.3ad;
• Possuir ferramenta de diagnóstico do tipo pcap;
• Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;
• Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
• Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.
• Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
• Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;
• Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
• Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;

• Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
• Deverá suportar aplicações multimídia como: H.323, SIP;
• Possuir tecnologia de firewall do tipo Stateful;
• Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo/passivo e ativo/ativo;
• Permitir o funcionamento em modo transparente tipo "bridge";
• Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;
• Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);
• Deverá suportar forwarding de multicast;
• Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP e UDP;
• Permitir o agrupamento de serviços;
• Permitir o filtro de pacotes sem a utilização de NAT;
• Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
• Possuir mecanismo de anti-spoofing;
• Permitir criação de regras definidas pelo usuário;
• Permitir o serviço de autenticação para HTTP e FTP;
• Possuir a funcionalidade de balanceamento e contingência de links;
• 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.
• Deve dar suporte e ter licenciada a virtualização de firewall, permitindo a criação de, no mínimo, 5 (cinco) firewalls virtuais (contextos ou domínios virtuais), onde cada um possa assumir logicamente em modo de NGFW e ainda possibilitar o uso de interfaces de redes, endereçamentos, políticas e roteamentos distintos.
• Todas as funcionalidades devem estar disponíveis em todos os contextos, não havendo limitações de uso quando sendo apenas o firewall base ou seus contextos virtualizados.
• Deve permitir a criação de administradores independentes, para cada um dos firewalls virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que possam ser administrados por equipes distintas.

1.10.2.4. IDENTIFICAÇÃO DO USUÁRIO

• Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;
• 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;
• 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;
• A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;
• 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;
• A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;

1.10.2.5. FUNCIONALIDADE DE REDE VIRTUAL PRIVADA (VPN)

• VPN baseada em appliance;
• Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
• Suporte a certificados PKI X.509 para construção de vpns;
• Possuir suporte a vpns ipsec site-to-site:
• Criptografia, 3DES, AES128, AES256, AES-GCM-128
• Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
• Algoritmo Internet Key Exchange (IKE) versões I e II;
• AES 128 e 256 (Advanced Encryption Standard);
• Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14;
• Deve permitir a arquitetura de vpn hub and spoke;

• Suporte a vpns ipsec client-to-site;
• Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);
• Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicosentre múltiplos dispositivos (spokes) com um gateway centralizador (hub).

1.10.2.6. FUNCIONALIDADE DO SISTEMA DE DETECÇÃO DE INTRUSÃO - IPS/IDS

• A Detecção de Intrusão deverá ser baseada em appliance;
• Possuir no mínimo 7.000 assinaturas ou regras de IPS/IDS;
• O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
• Possuir tecnologia de detecção baseada em assinatura;
• Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo bypass;
• O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;
• Possuir opção para administrar as listas de Blacklist, Whitelist e Quarentena com suporte a endereços ipv6;
• 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;
• Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (dos) do tipo Flood, Prot Scan e Sweep;
• Mecanismos de detecção/proteção de ataques;
• Reconhecimento de padrões;
• Análise de protocolos;
• Detecção de anomalias;
• Detecção de ataques de RPC (Remote procedure call);
• Proteção contra ataques de Windows ou netbios;
• Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
• Proteção contra ataques DNS (Domain Name System);
• Proteção contra ataques a FTP, SSH , Telnet e rlogin;
• Proteção contra ataques de ICMP (Internet Control Message Protocol);
• Alertas via correio eletrônico;
• 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;
• Capacidade de resposta ativa a ataques;
• Terminação de sessões via TCP resets;
• Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
• O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
• Possuir filtros de ataques por anomalias;
• Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
• Permitir filtros de anomalias de protocolos;
• Suportar reconhecimento de ataques de dos, reconnaissance, exploits e evasion;
• Suportar verificação de ataque nas camadas de aplicação;

1.10.2.7. FUNCIONALIDADE DE QoS

• Adotar solução de Qualidade de Serviço baseada em appliance;
• 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;
• Permitir modificação de valores DSCP;
• Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;
• Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

• Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
• Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
• Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
• Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

1.10.2.8. FUNCIONALIDADE DO ANTIVÍRUS

• Possuir funções de Antivírus, Anti-spyware;
• Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;
• Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);
• Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

1.10.2.9. FUNCIONALIDADE DO PROXY E FILTRO DE CONTEÚDO

• Possuir solução de filtro de conteúdo web integrado a solução de segurança;
• Possuir pelo menos 85 categorias para classificação de sites web;
• Possuir base mínima contendo, 1 milhão de sites internet web já registrados e classificados;
• 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;
• Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
• Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;
• Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;
• Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;
• Possibilitar a integração com servidores de cache WEB externos;
• Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®;
• 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;
• Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
• Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
• 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;
• Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
• Permitir a criação de listas personalizadas de urls permitidas – lista branca e bloqueadas – lista negra;
• Deverá permitir o bloqueio de urls inválidas cujo campo CN do certificado SSL não contém um domínio válido;
• Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
• Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
• Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
• Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
• Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
• Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e urls originadas de Spam;
• Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;

• Deverá permitir configurar a porta do Proxy Explícito.

1.10.2.10. FUNCIONALIDADE DO CONTROLE DE APLICAÇÕES

• As funcionalidades abaixo devem ser baseadas em Appliance:

• Reconhecer pelo menos 3.000 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/Video ou Audio, proxy ou tunelamento, mensagens instantâneas ou colaboração, compartilhamento de arquivos/storage, backup, mail;

• Reconhecer pelo menos as seguintes aplicações: 4Shared, Active Directory/SMB, Citrix ICA, DHCP Protocol, 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;

• 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, Vídeo Streaming/Play, Upload);

• Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

• 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, port hopping e túnel através de tráfego SSL encriptado;

• Atualizar a base de assinaturas de aplicações automaticamente;

• Reconhecer aplicações em ipv6;

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

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

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

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

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

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

• Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;

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

1.10.2.11. SISTEMA DE PROTEÇÃO ACANÇADA CONTRA AMEAÇAS - ATP

• Possuir sistema de proteção avançada contra ameaças (ATP) nativo;

• 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;

• 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;

• A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;

• Deve permitir a identificação de aplicativos e ameaças independente das portas e protocolos;

• 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;

• Deve permitir a atualização automática das assinaturas por meio de agendamento diário;

• Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, ataques P2P, trojans, worms, malwares para mobile, blacklist, vulnerabilidades conhecidas;

• Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus

e Antimalware;

• Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, ataques P2P, trojans, worms, malwares para mobile, blacklist, vulnerabilidades conhecidas;

• Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de voip tais como: Hotline, SIP, Skype;

• 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;

• Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: bittorrent, Gnutella, Napster e de Storages, tais como: Dropbox, Google Drive, Mega e onedrive;

• Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

• Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;

• Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as "ameaças detectadas" e as "ameaças bloqueadas";

• Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "aplicativos detectados" e os "aplicativos bloqueados";

• Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";

• 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.

1.10.2.12. SD-WAN (GERÊNCIA DE WAN)

• 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;

• Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;

• Permitir utilizar VPN ipsec para interligar unidades remotas;

• Possuir recurso de "persistência de link" para impedir a queda de conexões em aplicações que não suportam o load balance de link;

• 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;

• Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos relacionado ao recurso SD-WAN;

• Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações: Consumo de banda; Perda de pacotes; Jitter; Latência.

1.10.2.13. ALTA DISPONIBILIDADE

• Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Passivo ou Ativo/Ativo, com as implementações de Fail Over;

• 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;

• O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat.

1.10.2.14. REDUNDÂNCIA PARA MÚLTIPLOS ISPs (Provedores)

• A solução proposta deve suportar o balanceamento de carga e redundância para pelo menos 2 (dois) links de Internet;

• A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação;

• A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP;

• A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway;

• A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego ipv4 e ipv6.

1.10.3. FERRAMENTA DE GESTÃO DE RELATÓRIOS

1.10.3.1. CARACTERÍSTICA DA FERRAMENTA

- Deve ser do tipo appliance virtual (VM)
- Possuir capacidade de recebimento de logs de pelo menos 10 mil dispositivos
- Possuir a capacidade de receber pelo menos 9 Gbits de logs diários
- Deverá ser compatível com ambiente VMware ESXi 6.5 e superior
- Deverá ser compatível com ambiente Microsoft Hyper-V 2016, 2019 e 2022
- Deverá ser compatível com ambiente Citrix XenServer 8.2 e superior e Open Source Xen 4.2.5
- Deverá ser compatível com ambiente KVM
- Deverá ser compatível com ambiente Nutanix AHV
- Deverá ser compatível com ambiente Amazon Web Services (AWS)
- Deverá ser compatível com ambiente Microsoft Azure.
- Deverá ser compatível com o ambiente Google Cloud (GCP)
- Deverá ser compatível com o ambiente Oracle Cloud Infrastructure (OCI)
- Deverá ser compatível com o ambiente Alibaba Cloud (AliCloud)
- Não deve possuir limite na quantidade de múltiplas vCPU
- Não deve possuir limite para suporte a expansão de memória RAM

1.10.3.2. REQUISITOS MÍNIMOS DE FUNCIONALIDADE

- Suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções
- Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento.
- Permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento.
- Suportar SNMP versão 2 e 3
- Permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.
- Permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.
- Permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH
- Possuir autenticação de usuários para acesso à plataforma via LDAP
- Possuir autenticação de usuários para acesso à plataforma via Radius
- Possuir autenticação de usuários para acesso à plataforma via TACACS +
- Possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico
- Possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas.
- Possuir geração de relatórios de tráfego em tempo real, em formato de gráfico
- Possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.
- Possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.
- Possuir visualização da quantidade de logs enviados de cada dispositivo monitorado
- Possuir mecanismos de apagamento automático para logs antigos.
- Permitir importação e exportação de relatórios
- Deve ter a capacidade de criar relatórios no formato HTML
- Deve ter a capacidade de criar relatórios em formato PDF
- Deve ter a capacidade de criar relatórios no formato XML
- Deve ter a capacidade de criar relatórios no formato CSV
- Deve permitir exportar os logs no formato CSV
- Deve gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.
- Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.
- A solução deve ter relatórios predefinidos
- Deve poder enviar automaticamente os logs para um servidor FTP externo para a solução
- A duplicação de relatórios existentes deve ser possível para edição posterior.

• Ter a capacidade de personalizar a capa dos relatórios obtidos.
• Permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.
• Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados.
• Ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas
• Deve ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real.
• Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo.
• Ter a capacidade de gerar e enviar relatórios periódicos automaticamente.
• Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.
• Permitir o envio por e-mail relatórios automaticamente.
• Deve permitir que o relatório seja enviado por email ao destinatário específico.
• Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.
• É necessário exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.
• Deve permitir o uso de filtros nos relatórios.
• Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.
• Permitir especificar o idioma dos relatórios criados
• Gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.
• Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.
• Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.
• Possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros.
• Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.
• Importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.
• Deve ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.
• Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.
• Deve ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.
• Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos
• Deve permitir visualizar em tempo real os logs recebidos.
• Deve permitir o encaminhamento de log no formato syslog.
• Deve permitir o encaminhamento de log no formato CEF (Common Event Format).
• Deve disponibilizar painel de operações SOC composto por widgets configuráveis, permitindo o monitoramento de eventos de segurança, ameaças, usuários, aplicações, tráfego de rede, VPN, redes sem fio, endpoints, indicadores operacionais da plataforma e demais informações provenientes dos dispositivos integrados, conforme as funcionalidades suportadas pela solução
• Suportar a configuração Master / Slave de alta disponibilidade na camada 3
• Gerar alertas de eventos a partir de logs recebidos
• Permitir a criação de incidentes a partir de alertas de eventos para o terminal
• Permitir a integração ao sistema de tickets do ServiceNow
• Incluir serviço Indicadores de Comprometimento (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredicto (classificação geral da ameaça), o número de ameaças detectadas.

- Deve permitir o suporte a logs na nuvem pública do Amazon S3
- Deve permitir o suporte a logs na nuvem pública do Microsoft Azure
- Permitir o suporte aos registros de nuvem pública do Gooogle Cloud
- Suportar o padrão SAML para autenticação do usuário administrador
- Relatórios de Firewall
- Deve ter um relatório de conformidade com o PCI DSS
- Possuir um relatório de uso do aplicativo SaaS
- Possuir um relatório de prevenção de perda de dados (DLP)
- Possuir um relatório de VPN
- Possuir um relatório IPS (Intruder Prevention System)
- Possuir um relatório de reputação do cliente
- Possuir um relatório de análise de segurança do usuário
- Possuir um relatório de análise de ameaças cibernéticas
- Possuir um breve relatório resumido diário de eventos e incidentes de segurança
- Possuir um relatório de tráfego DNS
- Possuir um relatório de tráfego de e-mail
- Possuir um relatório dos 10 principais aplicativos usados na rede
- Possuir um relatório dos 10 principais sites usados na rede
- Possuir um relatório de uso de mídia social

1.11. ACORDO DE NÍVEL DE SERVIÇO - SLA

1.11.1. A LICITANTE deverá providenciar os atendimentos dentro das regras estabelecidas nesta seção:

- suporte técnico prestado em horário comercial, de segunda a sexta-feira com os seguintes prazos:

a) o atendimento virtual (remoto) de até 30 minutos após a abertura do chamado;

b) o atendimento presencial (quando necessário) em até 04 horas úteis após a abertura do chamado;

1.12. SUPORTE TÉCNICO

1.12.1. A licitante deverá prover suporte técnico necessário para garantir o perfeito funcionamento da solução descrita neste termo, bem como zelar pela resolução de possíveis incidentes no nível de serviço exigido, visando a não interrupção dos serviços contratados.

1.12.2. A empresa licitante deverá fornecer no mínimo dois canais de suporte ao cliente, sendo ao menos um canal por via digital, sendo aceito sistema web, formulário em site, atendimento via Whatsapp ou outros similares, desde que, possuam a capacidade de registrar e emitir comprovante de abertura de chamado;

1.12.3. Toda solicitação de suporte emitida pela Prefeitura de Garibaldi deverá ser registrada e controlada através da Central de Suporte da licitante contendo, minimamente, os dados de data e horário da abertura do chamado, identificação do solicitante e do técnico que receberá o chamado para iniciar o atendimento.

1.12.4. Os custos de Suporte Técnico deverão estar incluídos e distribuídos nos preços unitários.

1.12.5. Serão consideradas como Suporte Técnico todas as atividades empreendidas pela licitante necessárias para assegurar o funcionamento dos equipamentos, com o objetivo de possibilitar a continuidade dos serviços instalados e de garantir a alta disponibilidade objetiva.

1.12.6. O Suporte Técnico deverá ser acionável e realizado de segunda a sexta, no horário das 08:00 às 11:30 horas e das 13:30 às 17:00 horas, compreendendo:

a) manutenção corretiva: série de procedimentos destinados a reparar e a corrigir os componentes dos equipamentos e serviços, sem ônus à Prefeitura de Garibaldi, mantendo seu pleno estado de funcionamento, removendo definitivamente os defeitos eventualmente apresentados;

b) manutenção adaptativa: série de procedimentos destinados a adequar os itens de configuração em razão de alterações no ambiente tecnológico que suporta os equipamentos e serviços devendo a licitante informar à Prefeitura de Garibaldi a necessidade de atualização de qualquer software relativo à solução de NGFW;

c) A sede/filial da licitante deverá estar localizada a no máximo 130 quilômetros do Centro Administrativo da prefeitura, viabilizando o prazo de atendimento presencial;

1.13. IMPLANTAÇÃO

1.13.1. A solução de NGFW atualmente existente no município é do fabricante FORTINET, utilizando o hardware "Fortigate 80F" com firmware na versão 7.4.12, o sistema de auditoria e gestão de relatórios está configurado em ambiente virtual, utilizando a plataforma Hyper-V da Microsoft;

1.13.2. O processo de implantação tem por objetivo a inserção do hardware e software na infraestrutura da PREFEITURA de forma que o resultado final seja uma solução de NGFW com as mesmas características de organização interna (regras de firewall, conexões com AD, interfaceamento, VLANS, etc.) da solução atual;

1.13.3. A PREFEITURA designará um profissional responsável para acompanhamento e fornecimento de todas as informações pertinentes à implantação;

1.13.4. Todas as atividades relativas à implantação deverão acontecer em dias úteis (SEGUNDA-SEXTA) no intervalo das 08:00 – 17:00hs, remotamente ou presencialmente, de acordo com a necessidade;

1.13.5. A LICITANTE deverá fornecer um plano de implantação contendo minimamente as etapas e prazos para ser atingidos até a conclusão da implantação e início da prestação do serviço. Este plano deverá ser submetido ao Departamento de T.I do município para avaliação e posterior liberação para início dos trabalhos de implantação;

1.13.5.1. Em caso da solução de NGFW ser do mesmo fabricante da solução atual do município, a LICITANTE poderá substituir o plano de implantação por acesso prévio à nova solução para avaliar a migração direta das configurações através da cópia/restauração do arquivo de configuração;

1.13.6. A solução a ser adquirida deverá ser configurada de maneira que não seja necessário aquisição de novo hardware ou software para o seu pleno funcionamento;

1.13.7. A solução a ser adquirida deverá ser configurada de maneira que não seja necessário alterações estruturais no formato de organização da floresta/domínio do Active Directory pertencente ao município de Garibaldi;

1.13.8. A LICITANTE deverá fornecer credenciais com permissões suficientes para que os técnicos do Município de Garibaldi consigam fazer o gerenciamento COMPLETO da solução, incluindo todas as áreas abrangentes ao funcionamento e layout de conexão, criação e alteração de usuários administradores;

1.14. O prazo de início será a partir da assinatura do contrato, momento a partir do qual a contratada estará autorizada a realizar a instalação, configuração e ativação dos serviços contratados.

1.15. Deverão ser fornecidos todo hardware e licenças para uso e atualização de todos os componentes de software, vacinas de antivírus/malwares, assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período vigente da locação;

1.16. Para os itens que representem bens materiais, a LICITANTE deverá fornecer produtos novos, sem uso anterior. Por cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento;

1.17. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-ofsale, 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;

1.18. Toda solução fornecida deverá estar coberta por danos causados por eventos de força maior, com origem elétrica ou do meio ambiente, devendo ser imediatamente substituído sem custos adicionais ao CONTRATANTE;

1.19. O prazo de entrega e ativação da solução é de 30 (trinta) dias corridos contados da data de emissão da ordem de compra;

1.20. A solução deverá ser entregue e configurada na Prefeitura Municipal de Garibaldi, localizada na Rua Júlio de Castilhos, 254, Bairro Centro, Garibaldi/RS.

1.21. O prazo de vigência da contratação será de até 12 (doze) meses, a contar da assinatura do contrato, podendo ser prorrogado sucessivamente por meio de Termo Aditivo, até atingir o limite máximo de 10 anos de vigência, nos limites do artigo 107 da Lei 14.133/2021, a critério da Secretaria Contratante.

1.22. Caso haja algum serviço em desacordo com as especificações constantes no Termo de Referência e na proposta ou que seja de péssima qualidade, deverão ser reparados no prazo de 15 (quinze) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das

penalidades. Neste caso, a nota fiscal será retida até que seja regularizada a pendência, sendo autorizado o pagamento após a liberação da pessoa responsável.

CLÁUSULA SEGUNDA – DO PREÇO E DO PAGAMENTO

2.1. A Contratante pagará à Contratada, pelo lote o valor total de R$..... ( ), conforme especificação dos objetos a seguir:

LOTE ÚNICO					
ITEM	**OBJETO**	**QTDE**	**UN**	**VALOR UNITÁRIO**	**VALOR TOTAL**
01	SERVIÇOS DE LOCAÇÃO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL – NGFW), COMPREENDENDO O FORNECIMENTO DE APPLIANCE EM HARDWARE DEDICADO, LICENCIAMENTO COMPLETO DE TODAS AS FUNCIONALIDADES DE SEGURANÇA, SUPORTE TÉCNICO, GARANTIA, ATUALIZAÇÕES DE FIRMWARE, ASSINATURAS DE SEGURANÇA (IPS, ANTIVÍRUS, ANTIMALWARE, FILTRO DE CONTEÚDO WEB, CONTROLE DE APLICAÇÕES E WEB APPLICATION FIREWALL – WAF), ALÉM DO SERVIÇO DE LOGGING ANALYTICS PARA ARMAZENAMENTO, PROCESSAMENTO E ANÁLISE DOS REGISTROS (LOGS) GERADOS PELO EQUIPAMENTO. 10GB/DIA	12	UN		
02	IMPLEMENTAÇÃO	01	UN		
				VALOR TOTAL DO LOTE R$	

2.2. Os pagamentos serão efetuados mensalmente até o 30º (trigésimo) dia, contado a partir do recebimento da respectiva nota fiscal no setor de empenhos, desde que haja a devida comprovação da prestação dos serviços, atestada pelo fiscal, conforme Calendário de Pagamentos a Fornecedores, correndo a despesa na:

ÓRGÃO 13 – SECRETARIA MUNICIPAL DE INOVAÇÃO E EMPREENDEDORISMO
UNIDADE 1 - SECRETARIA MUNICIPAL DE INOVAÇÃO E EMPREENDEDORISMO
23.691.0094.2084 - MANUTENÇÃO DOS SERVIÇOS DA SMIE
3.3.9.04 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – (1340)
3.3.9.04.01.30 - COMUNICAÇÃO DE DADOS – (134013)

2.3. A forma de pagamento será por meio de crédito em conta bancária, devendo a contratada informar banco, agência, operação e número da conta bancária em nome da contratada, ou através de boleto de cobrança bancária.

a) Quando a cobrança ocorrer por boleto, o mesmo somente poderá ser emitido com código de barra padrão FEBRABAN com vencimento apresentação.

2.4. Caso o objeto do certame seja passível de retenção de imposto, conforme IN/RFB 1234/12 e IN/RFB 971/09, a contratada ficará sujeita à aplicação desta.

2.5. A nota fiscal/fatura emitida pelo fornecedor deverá conter, em local de fácil visualização, a indicação do nº do Pregão e da Ordem de Fornecimento, a fim de se acelerar o trâmite de recebimento do material e posterior liberação do documento fiscal para pagamento.

2.6. Na hipótese de existência de erros na nota fiscal de cobrança e/ou outra circunstância que impeça a liquidação da despesa, o pagamento será interrompido e ficará pendente até que a CONTRATADA adote as medidas saneadoras, voltando a correr na sua íntegra após a CONTRATADA ter solucionado o problema, seguindo a legislação vigente quanto à ordem cronológica de pagamentos do CONTRATANTE.

2.7. Em caso de atraso no pagamento por parte e por motivação da contratante, o valor devido será atualizado monetariamente com base no IPCA (IBGE), considerando-se a variação no período compreendido entre a data do vencimento e a data do efetivo pagamento.

CLÁUSULA TERCEIRA – DO VENCIMENTO DO CONTRATO, DO REAJUSTE, REPACTUAÇÃO E REEQUILÍBRIO

3.1. O prazo de vigência da contratação será de até 12 (doze) meses, a contar da assinatura do contrato, podendo ser prorrogado sucessivamente por meio de Termo Aditivo, até atingir o limite máximo de 10 anos de vigência, nos limites do artigo 107 da Lei 14.133/2021, a critério da Secretaria Contratante.

3.1.1. A data base para contagem dos prazos contratuais será definida a partir da homologação da licitação e estará registrada no contrato firmado entre as partes.

3.2. O licitante vencedor receberá o termo de contrato ou o instrumento equivalente, preferencialmente via digital, para assinatura imediata, devendo devolver o documento no prazo máximo de 07 dias úteis do recebimento, podendo este prazo ser prorrogado 1 (uma) vez, por igual período, mediante solicitação da parte, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

3.3. Expirado o prazo sem assinatura, será facultado à Administração, convocar os licitantes remanescentes, na ordem de classificação, para a celebração do contrato nas condições propostas pelo licitante vencedor.

3.4. Decorrido o prazo de validade da proposta indicado no item 3.2. deste Edital, sem convocação para a contratação, ficarão os licitantes liberados dos compromissos assumidos.

3.5. Na hipótese de nenhum dos licitantes aceitar a contratação, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

a) Convocar os licitantes remanescentes para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário;

b) Adjudicar e celebrar o contrato nas condições ofertadas pelos licitantes remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

3.6. A recusa injustificada do adjudicatário em assinar o contrato ou o instrumento equivalente no prazo estabelecido pela Administração caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas, previstas neste edital, e à imediata perda da garantia de proposta em favor do órgão licitante.

3.7. A vencedora deverá observar durante a execução do contrato as normas técnicas aplicáveis ao serviço, bem como as normas de segurança do trabalho.

3.8. A vencedora deverá executar os serviços observando fielmente o Termo de Referência, inclusive em relação à qualidade dos materiais e ao cronograma de execução, e os termos da sua proposta.

3.9. A vencedora deverá manter, durante toda a execução contratual, todas as condições de habilitação e qualificação exigidas na licitação, inclusive quanto às contribuições para o FGTS e INSS relativa aos empregados utilizados na prestação do serviço, devendo apresentar mensalmente à Administração os comprovantes de pagamentos dos encargos trabalhistas e previdenciários.

3.10. Antes de formalizar ou prorrogar o prazo de vigência do contrato, a Administração verificará a regularidade fiscal do contratado, consultar o Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e o Cadastro Nacional de Empresas Punidas (Cnep), emitir as certidões negativas de inidoneidade, de impedimento e de débitos trabalhistas e juntá-las ao respectivo processo.

3.11. A gestão do presente contrato ou instrumento equivalente será feita pelo servidor DANIEL DECONTI, matrícula 5324, tendo como obrigação:

a) conferir a existência de empenho prévio à realização da despesa;

b) acompanhar a publicação tempestiva do extrato do contrato;

c) conferir a existência de designação de fiscal para o contrato celebrado pela Administração;

d) controlar os limites de acréscimo e de supressão nas obras, serviços ou compras, inclusive em atas de registro de preços, em conformidade com a legislação;

e) adotar as providências para a confecção tempestiva dos termos aditivos, quando for o caso, atendidas as formalidades previstas na legislação.

f) receber ou formular os pedidos de repactuação e de reequilíbrio econômico-financeiro, encaminhando-os para os órgãos competentes realizarem a análise correspondente, submetendo-os à autoridade;

g) deliberar sobre o pedido de substituição do responsável técnico, desde que este detenha experiência e qualificação equivalente ou superior ao substituído, a ser verificada de acordo com as regras do processo que deu origem à contratação;

h) examinar, periodicamente, a atualização e a adequação da documentação do contratado em relação às obrigações trabalhistas, previdenciárias e fiscais, notificando-o em caso de irregularidade, dando ciência à autoridade, sugerindo a aplicação de sanção e a rescisão contratual se persistir o descumprimento, observados ampla defesa e o contraditório;

i) manifestar-se sobre eventual pedido de subcontratação;

j) executar outras atividades determinadas pelo superior hierárquico.

3.12. O responsável pela fiscalização do contrato será o servidor MARCELO DE BORBA, matrícula 5.110, que terá como obrigação:

a) conhecer os termos do processo de contratação e as condições do contrato, em especial os prazos, os cronogramas, as obrigações das partes, os casos de rescisão, a existência de cláusula de modificação do preço, se for o caso, e as hipóteses de aditamento;

b) acompanhar e fiscalizar a execução da obra, do serviço ou do fornecimento de bens, em estrita observância ao edital e ao contrato;

c) juntar documentos, registrar telefonemas, fazer anotações, redigir atas de reunião, anexar correspondências, inclusive as eletrônicas, e quaisquer documentos relativos à execução do contrato, no processo de fiscalização;

d) registrar todas as ocorrências durante a execução do contrato, solicitando ao Departamento Jurídico a notificação por escrito do contratado, que deverá conter determinação para saneamento das faltas ou defeitos observados em prazo a ser estipulado de acordo com o caso concreto;

e) fazer cumprir fielmente as obrigações avençadas, relatando por escrito e sugerindo à autoridade superior a aplicação das sanções, na forma do edital e do contrato, no caso de inadimplência, garantindo ao contratado o direito de defesa;

f) conferir a conclusão das etapas e o cumprimento das condições de pagamento;

g) dar recebimento provisório das obras, serviços e compras mediante termo circunstanciado;

h) dar recebimento definitivo das obras, serviços e compras mediante termo circunstanciado, se houver previsão expressa na portaria de designação; e

i) executar outras atividades determinadas pelo superior hierárquico.

3.13. A extinção do contrato poderá ser:

a) determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;

b) consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

c) determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

3.14. DO REAJUSTE/REEQUILÍBRIO/REPACTUAÇÃO

3.14.1. No vencimento do contrato os preços poderão ser reajustados, se for o caso, até o índice do IPCA, com data-base vinculada à data do orçamento estimado, respeitado o interregno de um ano para concessão.

3.14.2. A contratada, em função da dinâmica do mercado, poderá solicitar a atualização dos preços vigentes, mediante solicitação à Administração Municipal, acompanhada de documentos que comprovem a procedência do pedido.

3.14.3. A atualização não poderá ultrapassar o preço praticado no mercado e deverá manter a diferença percentual apurada entre o preço originalmente constante da proposta e o preço de mercado vigente à época.

3.14.4. O pedido de reequilíbrio somente será analisado pela Administração Pública após a inequívoca comprovação da ocorrência do fato gerador que ensejou o alegado desequilíbrio no fluxo financeiro da Contratada.

3.14.5. Considerando-se que o equilíbrio exigido na relação contratual envolve uma contraposição entre encargos e vantagens, não serão concedidos reequilíbrios que ensejam impacto irrisório ao Contratante.

3.14.6. A base de cálculo do reajuste anual será o valor da proposta financeira apresentada, com o acréscimo, se houver, de eventuais correções inflacionárias decorrentes do decurso de prazo contratual, sendo descontada a porcentagem dos reequilíbrios concedidos durante a contratação.

3.14.7. Poderá haver repactuação sempre que houver regime de dedicação exclusiva de mão de obra ou predominância de mão de obra, mediante demonstração analítica da variação dos custos.

3.14.8. O pedido de repactuação deve solicitado pela CONTRATADA e observado o interregno

mínimo de 01 (um) ano contado da data da apresentação da proposta ou da data da última repactuação, competindo à CONTRATADA justificar e comprovar a variação dos custos, apresentando memória de cálculo e planilhas apropriadas para análise e posterior aprovação da CONTRATANTE;

3.14.9. A repactuação poderá ser dividida em tantas parcelas quantas forem necessárias, em respeito ao princípio da anualidade do reajustamento dos preços da contratação, podendo ser realizada em momentos distintos para discutir a variação de custos que tenham sua anualidade resultante em datas diferenciadas, tais como os custos decorrentes da mão de obra e os custos decorrentes dos insumos necessários à execução do serviço.

3.14.10. O interregno mínimo de 01 (um) ano para a primeira repactuação será contado:

3.14.10.1. Para os custos relativos à mão de obra, vinculados à data-base da categoria profissional: a partir dos efeitos financeiros do acordo, dissídio ou convenção coletiva de trabalho, vigente à época da apresentação da proposta, relativo a cada categoria profissional abrangida pelo contrato;

3.14.10.2. Para os insumos discriminados na Planilha de Custos e Formação de Preços que estejam diretamente vinculados ao valor de preço público (tarifa): do último reajuste aprovado por autoridade governamental ou realizado por determinação legal ou normativa;

3.14.10.3. Para os demais custos, sujeitos à variação de preços do mercado (insumos não decorrentes da mão de obra): a partir da data limite para apresentação das propostas constantes do Edital.

3.14.11. Nas repactuações subsequentes à primeira, o interregno de um ano será computado da última repactuação correspondente à mesma parcela objeto de nova solicitação. Entende-se como última repactuação, a data em que iniciados seus efeitos financeiros, independentemente daquela em que celebrada ou apostilada.

3.14.12. O prazo para a CONTRATADA solicitar a repactuação encerra-se na data da prorrogação contratual subsequente ao novo acordo, dissídio ou convenção coletiva que fixar os novos custos de mão de obra da categoria profissional abrangida pelo contrato, ou na data do encerramento da vigência do contrato, caso não haja prorrogação.

3.14.13. Caso a CONTRATADA não solicite a repactuação tempestivamente, dentro do prazo acima fixado, ocorrerá a preclusão do direito à repactuação.

3.14.14. Nessas condições, se a vigência do contrato tiver sido prorrogada, nova repactuação só poderá ser pleiteada após o decurso de novo interregno mínimo de 01 (um) ano, contado:

3.14.14.1. Da vigência do acordo, dissídio ou convenção coletiva anterior, em relação aos custos decorrentes de mão de obra;

3.14.14.2. Do último reajuste aprovado por autoridade governamental ou realizado por determinação legal ou normativa, para os insumos discriminados na Planilha de Custos e Formação de Preços que estejam diretamente vinculados ao valor de preço público (tarifa); e

3.14.14.3. Do dia em que se completou um ou mais anos da apresentação da proposta, em relação aos custos sujeitos à variação de preços do mercado;

3.14.15. Caso, na data da prorrogação contratual, ainda não tenha sido celebrado o novo acordo, dissídio ou convenção coletiva da categoria, ou ainda não tenha sido possível à CONTRATANTE ou à CONTRATADA proceder aos cálculos devidos, deverá ser inserida cláusula no termo aditivo de prorrogação para resguardar o direito futuro à repactuação, a ser exercido tão logo se disponha dos valores reajustados, sob pena de preclusão.

3.14.16. A repactuação de preços será formalizada por apostilamento ou termo aditivo.

OBSERVAÇÃO: o prazo para resposta ao pedido de repactuação de preços será, preferencialmente de 1 (um) mês, contado da data do fornecimento da documentação.

CLÁUSULA QUARTA – DO PRAZO, LOCAL E CONDIÇÕES DE RECEBIMENTO

4.1. O prazo de vigência da contratação será de até 12 (doze) meses, a contar da assinatura do contrato, podendo ser prorrogado sucessivamente por meio de Termo Aditivo, até atingir o limite máximo de 10 anos de vigência, nos limites do artigo 107 da Lei 14.133/2021, a critério da Secretaria Contratante.

4.1.1. A data base para contagem dos prazos contratuais será definida a partir da homologação da licitação e estará registrada no contrato firmado entre as partes.

4.2. A aceitação do objeto somente será efetivada após ter sido o mesmo considerado satisfatório, pela fiscalização do(s) contrato(s), ficando a empresa fornecedora obrigada a substituí-lo, em parte ou integralmente, em tempo hábil, sempre que ocorrerem falhas.

4.3. O objeto da presente licitação será recebido:

4.3.1. Provisoriamente, para efeito de posterior verificação de sua conformidade com a especificação;

4.3.2. Definitivamente, após a verificação da qualidade e especificações do mesmo.

4.3.3. Serão rejeitados, por ocasião do recebimento definitivo, o objeto fornecido com as especificações diferentes das contidas no objeto e das informações na proposta.

4.4. Constatadas irregularidades quanto à especificação do objeto, o Município poderá rejeitá-lo, no todo ou em parte, determinando sua substituição (através de notificação, que poderá ser procedida por e-mail) ou rescindindo a contratação, sem prejuízo das penalidades cabíveis. Na hipótese de substituição, a licitante deverá fazê-la em conformidade com a indicação da Administração, **em prazo a ser definido na notificação**, mantido o preço inicialmente contratado, sob o risco de sofrer as penalidades constantes neste edital.

4.5. O recebimento provisório ou definitivo não exclui a responsabilidade da licitante vencedora pela perfeita execução do objeto, ficando a mesma obrigada a substituir, no todo ou em parte, se a qualquer tempo se verificar vícios, defeitos ou incorreções.

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

4.6.1. não produzir os resultados acordados,

4.6.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

4.6.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do contrato, ou utilizá-los com qualidade ou quantidade inferior à demandada.

CLÁUSULA QUINTA – DAS OBRIGAÇÕES

5.1. Das obrigações da CONTRATADA:

a) prestar os serviços de acordo com as especificações do contrato e as solicitações da Administração;

b) disponibilizar veículos em perfeitas condições de uso, conservação, limpeza, segurança e regularidade perante os órgãos competentes;

c) disponibilizar motoristas devidamente habilitados e qualificados para a condução dos veículos;

d) manter frota e estrutura operacional suficientes para atender às demandas simultâneas da Administração;

e) arcar com todas as despesas decorrentes da execução do contrato, incluindo combustível, manutenção preventiva e corretiva, tributos, seguros, encargos trabalhistas, previdenciários e demais custos;

f) responder por quaisquer danos causados ao Município, aos usuários ou a terceiros em decorrência da execução dos serviços;

g) manter, durante toda a vigência contratual, as condições de habilitação e qualificação exigidas na licitação;

h) comunicar imediatamente à Administração qualquer ocorrência que possa comprometer a execução dos serviços;

5.2. DO MUNICÍPIO:

a) Prestar informações e os esclarecimentos atinentes ao objeto, que venham a ser solicitados pela licitante;

b) Efetuar o pagamento nas condições e preços pactuados;

c) Fiscalizar a execução do objeto do contrato por meio de servidor designado;

CLÁUSULA SEXTA – DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. O responsável pela fiscalização do contrato será o servidor MARCELO DE BORBA, matrícula 5.110.

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

CLÁUSULA SÉTIMA – DA RESCISÃO

7.1. O CONTRATANTE poderá rescindir o presente contrato independente de interpelação ou de procedimento judicial:

7.1.1. no caso de dolo, culpa, simulação ou fraude na execução do contrato.

7.1.2. se a CONTRATADA transferir o contrato ou sua execução no todo ou em parte sem prévia autorização do CONTRATANTE.

7.1.3. se a CONTRATADA falir, entrar em concordata / recuperação judicial, em liquidação ou dissolução, e ainda alteração em sua estrutura social, que impossibilite ou prejudique a execução dos serviços.

7.1.4. O descumprimento de qualquer encargo trabalhista com os funcionários contratados pela Contratada. Será também aplicada advertência, multa de 10% do valor do contrato e poderá ser suspensa de participar em licitações com esta administração.

7.1.5. A CONTRATADA poderá rescindir o contrato quando o CONTRATANTE não efetuar os pagamentos que lhe são devidos no prazo de 60 (sessenta) dias.

7.1.6. O contrato poderá ser rescindido, ainda, por acordo mútuo, atendida a conveniência dos serviços, recebendo a CONTRATADA o valor dos serviços devidamente executados.

7.1.7. Em caso de inadimplemento contratual, por qualquer das partes, que resulte em rescisão contratual, estarão ambas as partes sujeitas às consequências da Lei nº 14.133/21.

CLÁUSULA OITAVA – DAS PENALIDADES

8.1. O licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações:

8.1.1. Dar causa à inexecução parcial do contrato;

8.1.2. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

8.1.3. Dar causa à inexecução total do contrato;

8.1.4. Deixar de entregar a documentação exigida para o certame;

8.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

8.1.7. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

8.1.8. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

8.1.9. Fraudar a licitação ou praticar ato fraudulento na execução do contrato;

8.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

8.1.11. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

8.1.12. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

8.2. Serão aplicadas ao responsável pelas infrações administrativas previstas cláusula sétima deste contrato as seguintes sanções:

8.2.1. Advertência;

8.2.2. Multa de no mínimo 0,5% (cinco décimos por cento) e máximo de 30% (trinta por cento)

do valor do objeto licitado ou contratado;

8.2.3. Impedimento de licitar e contratar, no âmbito da Administração Pública direta e indireta do órgão licitante, pelo prazo máximo de 3 (três) anos.

8.2.4. Declaração de inidoneidade para 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.

8.3. As sanções previstas poderão ser aplicadas cumulativamente.

8.4. A aplicação de multa de mora não impedirá que a Administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções.

8.5. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será cobrada judicialmente.

8.6. A aplicação das sanções previstas deste Edital não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

8.7. Na hipótese de deferimento de pedido de produção de novas provas ou de juntada de provas julgadas indispensáveis pela comissão, o licitante ou o contratado poderá apresentar alegações finais no prazo de 15 (quinze) dias úteis, contado da data da intimação.

8.8. Serão indeferidas pela comissão, mediante decisão fundamentada, provas ilícitas, impertinentes, desnecessárias, protelatórias ou intempestivas.

8.9. A personalidade jurídica poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos nesta Lei ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

8.10. É admitida a reabilitação do licitante ou contratado perante a própria autoridade que aplicou a penalidade, exigidos, cumulativamente:

8.10.1. Reparação integral do dano causado à Administração Pública;

8.10.2. Pagamento da multa;

8.10.3. Transcurso do prazo mínimo de 1 (um) ano da aplicação da penalidade, no caso de impedimento de licitar e contratar, ou de 3 (três) anos da aplicação da penalidade, no caso de declaração de inidoneidade;

8.10.4. Cumprimento das condições de reabilitação definidas no ato punitivo;

8.10.5. Análise jurídica prévia, com posicionamento conclusivo quanto ao cumprimento dos requisitos definidos neste artigo.

CLÁUSULA NONA – DAS DISPOSIÇÕES GERAIS

9.1. Para dirimir quaisquer divergências oriundas do presente contrato, casos omissos ou fortuitos, as partes contratantes elegem o foro da Comarca de GARIBALDI/RS, renunciando a qualquer outro.

9.2. E por estarem justos e contratados, assinam eletronicamente o presente contrato, por si e seus sucessores, em conformidade com a legislação vigente, considerando que todas as vias eletrônicas possuem a mesma validade jurídica para todos os fins de direito.

Garibaldi/RS, XX de XX de 2026.

Município de Garibaldi/RS Sérgio Chesini	Contratada CNPJ
Ass. jurídica	Fiscal

Este contrato foi examinado e aprovado por esta Assessoria Jurídica.

RIDAN COSER VILLA – OAB/RS 132.546
ssessor Jurídico/Procuradoria Geral do Município

A N E X O V – TERMO DE REFERÊNCIA
PREGÃO Nº ___/2026

TERMO DE REFERÊNCIA

SECRETARIA: SECRETARIA MUNICIPAL DE INOVAÇÃO E EMPREENDEDORISMO
OBJETO: CONTRATAÇÃO DE EMPRESA PARA A PRESTAÇÃO DE SERVIÇO DE LOCAÇÃO DE "APPLIANCE DE FIREWALL NEXT GENERATION" - NGFW

1. DEFINIÇÃO DO OBJETO

1.1. O presente Termo de Referência tem por objeto a contratação de empresa especializada para a locação de solução de Firewall de Próxima Geração (Next Generation Firewall – NGFW), por meio de appliance em hardware dedicado, incluindo o fornecimento dos equipamentos, licenciamento integral de todas as funcionalidades, instalação, configuração, migração da solução atualmente em operação, suporte técnico especializado, garantia, manutenção corretiva, atualização de firmware e de assinaturas de segurança, bem como todos os demais serviços necessários ao pleno funcionamento da solução durante toda a vigência contratual.

LOTE ÚNICO					
ITEM	**DESCRIÇÃO**	**UNID**	**QUANT**	**VALOR MENSAL**	**TOTAL**
1	SERVIÇOS DE LOCAÇÃO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL – NGFW), COMPREENDENDO O FORNECIMENTO DE APPLIANCE EM HARDWARE DEDICADO, LICENCIAMENTO COMPLETO DE TODAS AS FUNCIONALIDADES DE SEGURANÇA, SUPORTE TÉCNICO, GARANTIA, ATUALIZAÇÕES DE FIRMWARE, ASSINATURAS DE SEGURANÇA (IPS, ANTIVÍRUS, ANTIMALWARE, FILTRO DE CONTEÚDO WEB, CONTROLE DE APLICAÇÕES E WEB APPLICATION FIREWALL – WAF), ALÉM DO SERVIÇO DE LOGGING ANALYTICS PARA ARMAZENAMENTO, PROCESSAMENTO E ANÁLISE DOS REGISTROS (LOGS) GERADOS PELO EQUIPAMENTO. 10GB/DIA	MESES	12	R$ 7.240,66	R$ 86.887,92
2	IMPLEMENTAÇÃO	UNI.	01	R$ 23.307,47	R$ 23.307,47

1.2. O objeto desta contratação não se enquadra como bem de luxo, conforme Decreto Municipal nº 4.765/2023, caracterizando-se como comum, de acordo com justificativa constante no Estudo Técnico Preliminar.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. Com o aumento exponencial de ameaças cibernéticas e a crescente complexidade dos ambientes de TI, torna-se imprescindível adotar soluções de segurança capazes de oferecer proteção avançada contra ataques sofisticados, bem como, oferecer recursos internos para proteção dos dados em consonância com leis de proteção de dados e a Política de Segurança da Informação do Município de Garibaldi. Os firewalls tradicionais, focados apenas em filtragem de pacotes e controle de portas/protocolos, já não atendem a estas demandas segurança corporativa presentes no dia a dia.

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

2.2. O uso de um Firewall de Próxima Geração (NGFW) propicia a inspeção profunda de pacotes, prevenção contra intrusões, controle de aplicações – locais e em nuvem, além de oferecer segurança integrada com uma gestão eficiente através de console centralizado e relatórios avançados.

2.3. Com a manutenção desta solução, espera-se a redução significativa dos riscos de ataques cibernéticos, maior proteção de dados, continuidade de serviços e acesso à nuvem, otimização da gestão da segurança com monitoramento em tempo real, e por fim – conformidade com a legislação e regulamentações internas pertinentes à área.

2.4. O levantamento de mercado realizado durante a fase de planejamento identificou que a contratação de soluções de Firewall de Próxima Geração (NGFW) é prática consolidada na Administração Pública, existindo diversos órgãos que realizaram licitações com objeto semelhante, contemplando fornecimento de appliance, licenciamento, implantação, migração, treinamento, suporte técnico e atualização das assinaturas de segurança. Entre eles destacam-se a **Casa da Moeda do Brasil**, a **Secretaria de Estado de Planejamento e Administração do Pará (SEPLAD/PA)**, a **Escola Superior do Ministério Público da União (ESMPU)**, a **Comissão de Valores Mobiliários (CVM)** e a contratação centralizada promovida pelo **Ministério da Gestão e da Inovação em Serviços Públicos (MGI)** para fornecimento de soluções NGFW aos órgãos da Administração Pública Federal, evidenciando que o objeto possui ampla oferta no mercado e especificações técnicas padronizadas.

2.5. A contratação se mostra ainda coerente com os princípios da economicidade, planejamento, transparência e interesse público, contribuindo para a melhoria da prestação dos serviços públicos e para a segurança das informações institucionais.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

3.1. A solução de NGFW a ser fornecida através de "*appliance*" com capacidade de Inspeção profunda de pacotes (DPI), análise detalhada do tráfego para identificar ameaças ocultas, prevenção contra intrusões (IPS/IDS) e bloqueio proativo de tentativas de exploração de vulnerabilidades, além de oferecer a possibilidade de auditoria dos acessos realizados através da emissão e gestão de relatórios especializados.

3.2. A solução deverá atuar como principal mecanismo de proteção do perímetro da rede corporativa e da rede interna da Administração Municipal, realizando inspeção, monitoramento e controle de todo o tráfego de dados entre a rede interna e a Internet, bem como entre segmentos internos da infraestrutura tecnológica, prevenindo acessos não autorizados, ataques cibernéticos e demais ameaças que possam comprometer a disponibilidade, integridade e confidencialidade das informações.

3.3. A solução deverá contemplar, no mínimo, funcionalidades de Firewall Stateful, inspeção profunda de pacotes (Deep Packet Inspection – DPI), controle de aplicações por camada 7 (Layer 7), identificação de usuários, administração de largura de banda (QoS), VPN IPsec, Sistema de Prevenção e Detecção de Intrusão (IPS/IDS), proteção contra vírus, malwares e demais códigos maliciosos, filtro de conteúdo web, inspeção de tráfego criptografado (SSL Inspection), proteção de aplicações web (Web Application Firewall – WAF), geração de relatórios especializados e mecanismos avançados de auditoria dos acessos realizados.

3.4. A solução deverá incluir serviço de Logging Analytics, responsável pelo armazenamento, indexação, pesquisa e análise dos registros de eventos (logs) gerados pelo equipamento, permitindo a rastreabilidade das ações realizadas na rede, emissão de relatórios gerenciais, auditoria de eventos de segurança e apoio às

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

atividades de monitoramento e resposta a incidentes. A capacidade mínima contratada deverá ser de 10 GB de ingestão de logs por dia, atendendo ao consumo atual da infraestrutura municipal e prevendo margem para o crescimento da demanda durante a vigência contratual.

3.5. Também deverão integrar a contratação todas as licenças necessárias ao funcionamento integral da solução, incluindo atualizações de firmware, assinaturas de antivírus, antimalware, IPS, filtro de conteúdo web, controle de aplicações, Web Application Firewall (WAF) e demais componentes de segurança, sem qualquer custo adicional para a Administração durante todo o período da locação.

3.6. A contratada será responsável pela instalação física e lógica da solução, configuração dos equipamentos, migração das políticas de segurança atualmente existentes, integração com o ambiente de auditoria e gerenciamento de logs já implantado pelo Município, realização de testes de funcionamento, homologação da solução, treinamento operacional da equipe técnica e prestação de suporte técnico especializado durante toda a vigência do contrato.

3.7. A solução deverá ser compatível com instalação em rack padrão de 19 polegadas, conforme norma EIA-310, ocupando no máximo 1U de altura, e deverá garantir níveis adequados de desempenho para suportar o volume de tráfego da rede municipal, assegurando a continuidade dos serviços públicos digitais e permitindo futuras expansões da infraestrutura tecnológica sem necessidade de substituição prematura da solução contratada.

3.8. Por se tratar de uma solução integrada de hardware, software, licenciamento e serviços especializados, todos os componentes deverão ser fornecidos por uma única contratada, garantindo total compatibilidade entre os equipamentos, funcionalidades e serviços prestados, bem como maior eficiência na gestão contratual, na manutenção da solução e na responsabilização técnica durante toda a execução do contrato.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Fornecimento de solução de NGFW com as seguintes características:

4.1.1. CARACTERÍSTICAS DO HARDWARE:

- O equipamento deve ser compatível com instalação em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45 mm);
- Dispor de pelo menos duas fontes de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz cada;
- Possuir painel ou led indicador on/off e devices de rede;
- Possuir throughput de no mínimo 26 Gbps para tráfego UDP independente do tamanho dos pacotes;
- Suportar no mínimo 2.900.000 (dois milhões e novecentas mil) conexões simultâneas;
- Suportar no mínimo 130.000 (cento e trinta mil) novas conexões por segundo;
- Possuir throughput mínimo de 5 Gbps para tráfego IPS/IDS;
- Possuir throughput mínimo de 30Gbps para tráfego VPN IPSEC;
- Possuir throughput mínimo de 3 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);
- Possuir pelo menos 16 (dezesseis) interfaces de rede Gigabit Ethernet 10/100/1000, as portas

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

- Possuir no mínimo 4 lans 10GBE SFP+;
- Possuir no mínimo 8 lans 1GBE SFP;
- Possuir no mínimo 1 (uma) porta console de conexão para acesso à interface de comando CLI específica para esta finalidade;
- Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos.

4.1.2. ESPECIFICAÇÃO GERAL DO SOFTWARE NGFW:

4.1.2.1. FUNÇÕES BÁSICAS

- Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;
- Agentless VPN, VPN ipsec (Client-to-site e Site-to-site);
- Controle de Aplicações;
- Proxy Web e Filtro de Conteúdo Web (URL Filtering);
- Detecção e prevenção de intrusos – IPS;
- Qualidade de serviço – QoS;
- Anti-Malware;
- SD-WAN;
- Cluster.

4.1.2.2. CARACTERÍSTICAS GERAIS

- Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui *stateful firewall* 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, IPS, prevenção contra ameaças de vírus, malwares, filtro de URL, inspeção de tráfego criptografado e proteção de firewall de aplicação Web.
- Interface em português e inglês;
- O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;
- Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução;
- A solução deverá ser em hardware dedicado tipo *appliance* com sistema operacional customizado para garantir segurança e melhor desempenho;
- Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;
- Não deve ser necessária a instalação de qualquer software no dispositivo cliente para realizar o acesso ou a administração dos recursos do equipamento, bem como adição e utilização de servidores e/ou appliances.

4.1.2.3. FUNCIONALIDADES DO FIREWALL

- Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

- Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;
- Deve possuir ferramentas para realizar backups de forma remota, por SSH, FTP, NFS ou próprio do fabricante. Deve também permitir backup em Pen-drive. A solução deve permitir o agendamento diário ou semanal do backup;
- Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.
- Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica;
- As cópias de segurança devem ser salvas criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;
- Deve permitir habilitar ou desabilitar o registro de log por política de firewall.
- Possuir controle de acesso à internet por endereço IP de origem e destino;
- Possuir controle de acesso à internet por sub-rede;
- Possuir suporte a tags de VLAN (802.1q);
- Suportar agregação de links, segundo padrão IEEE 802.3ad;
- Possuir ferramenta de diagnóstico do tipo pcap;
- Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;
- Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
- Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.
- Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
- Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;
- Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
- Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;
- Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- Deverá suportar aplicações multimídia como: H.323, SIP;
- Possuir tecnologia de firewall do tipo Stateful;
- Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo/passivo e ativo/ativo;
- Permitir o funcionamento em modo transparente tipo “bridge”;
- Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;
- Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);
- Deverá suportar forwarding de multicast;
- Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP e UDP;
- Permitir o agrupamento de serviços;
- Permitir o filtro de pacotes sem a utilização de NAT;

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

- Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- Possuir mecanismo de anti-spoofing;
- Permitir criação de regras definidas pelo usuário;
- Permitir o serviço de autenticação para HTTP e FTP;
- Possuir a funcionalidade de balanceamento e contingência de links;
- 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.
- Deve dar suporte e ter licenciada a virtualização de firewall, permitindo a criação de, no mínimo, 5 (cinco) firewalls virtuais (contextos ou domínios virtuais), onde cada um possa assumir logicamente em modo de NGFW e ainda possibilitar o uso de interfaces de redes, endereçamentos, políticas e roteamentos distintos.
- Todas as funcionalidades devem estar disponíveis em todos os contextos, não havendo limitações de uso quando sendo apenas o firewall base ou seus contextos virtualizados.
- Deve permitir a criação de administradores independentes, para cada um dos firewalls virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que possam ser administrados por equipes distintas.

4.1.2.4. IDENTIFICAÇÃO DO USUÁRIO

- Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;
- 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;
- 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;
- A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;
- 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;
- A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;

4.1.2.5. FUNCIONALIDADE DE REDE VIRTUAL PRIVADA (VPN)

- VPN baseada em appliance;
- Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- Suporte a certificados PKI X.509 para construção de vpns;
- Possuir suporte a vpns ipsec site-to-site:
- Criptografia, 3DES, AES128, AES256, AES-GCM-128
- Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
- Algoritmo Internet Key Exchange (IKE) versões I e II;
- AES 128 e 256 (Advanced Encryption Standard);

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

- Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14;
- Deve permitir a arquitetura de vpn hub and spoke;
- Suporte a vpns ipsec client-to-site;
- Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);
- Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).

4.1.2.5. FUNCIONALIDADE DO SISTEMA DE DETECÇÃO DE INTRUSÃO - IPS/IDS

- A Detecção de Intrusão deverá ser baseada em appliance;
- Possuir no mínimo 7.000 assinaturas ou regras de IPS/IDS;
- O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
- Possuir tecnologia de detecção baseada em assinatura;
- Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass;
- O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;
- Possuir opção para administrar as listas de Blacklist, Whitelist e Quarentena com suporte a endereços ipv6;
- 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;
- Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (dos) do tipo Flood, Prot Scan e Sweep;
- Mecanismos de detecção/proteção de ataques;
- Reconhecimento de padrões;
- Análise de protocolos;
- Detecção de anomalias;
- Detecção de ataques de RPC (Remote procedure call);
- Proteção contra ataques de Windows ou netbios;
- Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
- Proteção contra ataques DNS (Domain Name System);
- Proteção contra ataques a FTP, SSH , Telnet e rlogin;
- Proteção contra ataques de ICMP (Internet Control Message Protocol);
- Alertas via correio eletrônico;
- 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;
- Capacidade de resposta ativa a ataques;
- Terminação de sessões via TCP resets;
- Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

- O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
- Possuir filtros de ataques por anomalias;
- Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- Permitir filtros de anomalias de protocolos;
- Suportar reconhecimento de ataques de dos, reconnaissance, exploits e evasion;
- Suportar verificação de ataque nas camadas de aplicação;

4.1.2.6. FUNCIONALIDADE DE QoS

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

4.1.2.7. FUNCIONALIDADE DO ANTIVÍRUS

- Possuir funções de Antivírus, Anti-spyware;
- Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;
- Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);
- Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

4.1.2.8. FUNCIONALIDADE DO PROXY E FILTRO DE CONTEÚDO

- Possuir solução de filtro de conteúdo web integrado a solução de segurança;
- Possuir pelo menos 85 categorias para classificação de sites web;
- Possuir base mínima contendo, 1 milhão de sites internet web já registrados e classificados;
- 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;
- Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

- Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;
- Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;
- Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;
- Possibilitar a integração com servidores de cache WEB externos;
- Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®;
- 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;
- Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
- 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;
- Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
- Permitir a criação de listas personalizadas de urls permitidas – lista branca e bloqueadas – lista negra;
- Deverá permitir o bloqueio de urls inválidas cujo campo CN do certificado SSL não contém um domínio válido;
- Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
- Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
- Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e urls originadas de Spam;
- Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;
- Deverá permitir configurar a porta do Proxy Explícito.

4.1.2.9. FUNCIONALIDADE DO CONTROLE DE APLICAÇÕES

- As funcionalidades abaixo devem ser baseadas em Appliance:
- Reconhecer pelo menos 3.000 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/Video ou Audio, proxy ou tunelamento, mensagens instantâneas ou colaboração, compartilhamento de arquivos/storage, backup, mail;

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

- Reconhecer pelo menos as seguintes aplicações: 4Shared, Active Directory/SMB, Citrix ICA, DHCP Protocol, 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;
- 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, Vídeo Streaming/Play, Upload);
- Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 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, port hopping e túnel através de tráfego SSL encriptado;
- Atualizar a base de assinaturas de aplicações automaticamente;
- Reconhecer aplicações em ipv6;
- Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

4.1.2.10. SISTEMA DE PROTEÇÃO ACANÇADA CONTRA AMEAÇAS - ATP

- Possuir sistema de proteção avançada contra ameaças (ATP) nativo;
- 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;
- 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;
- A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;
- Deve permitir a identificação de aplicativos e ameaças independente das portas e protocolos;

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

- 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;
- Deve permitir a atualização automática das assinaturas por meio de agendamento diário;
- Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, ataques P2P, trojans, worms, malwares para mobile, blacklist, vulnerabilidades conhecidas;
- Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;
- Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, ataques P2P, trojans, worms, malwares para mobile, blacklist, vulnerabilidades conhecidas;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de voip tais como: Hotline, SIP, Skype;
- 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;
- Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: bittorrent, Gnutella, Napster e de Storages, tais como: Dropbox, Google Drive, Mega e onedrive;
- Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;
- Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;
- Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as “ameaças detectadas” e as “ameaças bloqueadas”;
- Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os “aplicativos detectados” e os “aplicativos bloqueados”;
- Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: “baixo; médio e alto”;
- 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.

4.1.2.11. SD-WAN (GERÊNCIA DE WAN)

- 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;
- Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;
- Permitir utilizar VPN ipsec para interligar unidades remotas;
- Possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link;
- O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;

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

4.1.2.12. ALTA DISPONIBILIDADE

- Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Passivo ou Ativo/Ativo, com as implementações de Fail Over;
- 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;
- O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat.

4.1.2.13. REDUNDÂNCIA PARA MÚLTIPLOS ISPs (Provedores)

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

4.1.3. FERRAMENTA DE GESTÃO DE RELATÓRIOS

4.1.3.1. CARACTERÍSTICA DA FERRAMENTA

- Deve ser do tipo appliance virtual (VM)
- Possuir capacidade de recebimento de logs de pelo menos 10 mil dispositivos
- Possuir a capacidade de receber pelo menos 9 Gbits de logs diários
- Deverá ser compatível com ambiente VMware ESXi 6.5 e superior
- Deverá ser compatível com ambiente Microsoft Hyper-V 2016, 2019 e 2022
- Deverá ser compatível com ambiente Citrix XenServer 8.2 e superior e Open Source Xen 4.2.5
- Deverá ser compatível com ambiente KVM
- Deverá ser compatível com ambiente Nutanix AHV
- Deverá ser compatível com ambiente Amazon Web Services (AWS)
- Deverá ser compatível com ambiente Microsoft Azure.
- Deverá ser compatível com o ambiente Google Cloud (GCP)
- Deverá ser compatível com o ambiente Oracle Cloud Infrastructure (OCI)
- Deverá ser compatível com o ambiente Alibaba Cloud (AliCloud)

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

- Não deve possuir limite na quantidade de múltiplas vCPU
- Não deve possuir limite para suporte a expansão de memória RAM

4.1.3.2. REQUISITOS MÍNIMOS DE FUNCIONALIDADE

- Suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções
- Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento.
- Permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento.
- Suportar SNMP versão 2 e 3
- Permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.
- Permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.
- Permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH
- Possuir autenticação de usuários para acesso à plataforma via LDAP
- Possuir autenticação de usuários para acesso à plataforma via Radius
- Possuir autenticação de usuários para acesso à plataforma via TACACS +
- Possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico
- Possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas.
- Possuir geração de relatórios de tráfego em tempo real, em formato de gráfico
- Possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.
- Possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.
- Possuir visualização da quantidade de logs enviados de cada dispositivo monitorado
- Possuir mecanismos de apagamento automático para logs antigos.
- Permitir importação e exportação de relatórios
- Deve ter a capacidade de criar relatórios no formato HTML
- Deve ter a capacidade de criar relatórios em formato PDF
- Deve ter a capacidade de criar relatórios no formato XML
- Deve ter a capacidade de criar relatórios no formato CSV
- Deve permitir exportar os logs no formato CSV
- Deve gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.
- Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.
- A solução deve ter relatórios predefinidos
- Deve poder enviar automaticamente os logs para um servidor FTP externo para a solução

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

- A duplicação de relatórios existentes deve ser possível para edição posterior.
- Ter a capacidade de personalizar a capa dos relatórios obtidos.
- Permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.
- Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados.
- Ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas
- Deve ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real.
- Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo.
- Ter a capacidade de gerar e enviar relatórios periódicos automaticamente.
- Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.
- Permitir o envio por e-mail relatórios automaticamente.
- Deve permitir que o relatório seja enviado por email ao destinatário específico.
- Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.
- É necessário exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.
- Deve permitir o uso de filtros nos relatórios.
- Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.
- Permitir especificar o idioma dos relatórios criados
- Gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.
- Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.
- Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.
- Possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros.
- Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.
- Importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.
- Deve ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.
- Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.
- Deve ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.
- Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

- Deve permitir visualizar em tempo real os logs recebidos.
- Deve permitir o encaminhamento de log no formato syslog.
- Deve permitir o encaminhamento de log no formato CEF (Common Event Format).
- Deve disponibilizar painel de operações SOC composto por widgets configuráveis, permitindo o monitoramento de eventos de segurança, ameaças, usuários, aplicações, tráfego de rede, VPN, redes sem fio, endpoints, indicadores operacionais da plataforma e demais informações provenientes dos dispositivos integrados, conforme as funcionalidades suportadas pela solução
- Suportar a configuração Master / Slave de alta disponibilidade na camada 3
- Gerar alertas de eventos a partir de logs recebidos
- Permitir a criação de incidentes a partir de alertas de eventos para o terminal
- Permitir a integração ao sistema de tickets do ServiceNow
- Incluir serviço Indicadores de Comprometimento (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredicto (classificação geral da ameaça), o número de ameaças detectadas.
- Deve permitir o suporte a logs na nuvem pública do Amazon S3
- Deve permitir o suporte a logs na nuvem pública do Microsoft Azure
- Permitir o suporte aos registros de nuvem pública do Gooogle Cloud
- Suportar o padrão SAML para autenticação do usuário administrador
- Relatórios de Firewall
- Deve ter um relatório de conformidade com o PCI DSS
- Possuir um relatório de uso do aplicativo SaaS
- Possuir um relatório de prevenção de perda de dados (DLP)
- Possuir um relatório de VPN
- Possuir um relatório IPS (Intruder Prevention System)
- Possuir um relatório de reputação do cliente
- Possuir um relatório de análise de segurança do usuário
- Possuir um relatório de análise de ameaças cibernéticas
- Possuir um breve relatório resumido diário de eventos e incidentes de segurança
- Possuir um relatório de tráfego DNS
- Possuir um relatório de tráfego de e-mail
- Possuir um relatório dos 10 principais aplicativos usados na rede
- Possuir um relatório dos 10 principais sites usados na rede
- Possuir um relatório de uso de mídia social

4.2. ACORDO DE NÍVEL DE SERVIÇO - SLA

4.2.1. A LICITANTE deverá providenciar os atendimentos dentro das regras estabelecidas nesta seção:

- suporte técnico prestado em horário comercial, de segunda a sexta-feira com os seguintes prazos:
    - atendimento virtual (remoto) de até 30 minutos após a abertura do chamado;

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

- atendimento presencial (quando necessário) em até 04 horas úteis após a abertura do chamado;

4.3. SUPORTE TÉCNICO

4.3.1. A licitante deverá prover suporte técnico necessário para garantir o perfeito funcionamento da solução descrita neste termo, bem como zelar pela resolução de possíveis incidentes no nível de serviço exigido, visando a não interrupção dos serviços contratados.

4.3.2. A empresa licitante deverá fornecer no mínimo dois canais de suporte ao cliente, sendo ao menos um canal por via digital, sendo aceito sistema web, formulário em site, atendimento via Whatsapp ou outros similares, desde que, possuam a capacidade de registrar e emitir comprovante de abertura de chamado;

4.3.3. Toda solicitação de suporte emitida pela Prefeitura de Garibaldi deverá ser registrada e controlada através da Central de Suporte da licitante contendo, minimamente, os dados de data e horário da abertura do chamado, identificação do solicitante e do técnico que receberá o chamado para iniciar o atendimento.

4.3.4. Os custos de Suporte Técnico deverão estar incluídos e distribuídos nos preços unitários.

4.3.5. Serão consideradas como Suporte Técnico todas as atividades empreendidas pela licitante necessárias para assegurar o funcionamento dos equipamentos, com o objetivo de possibilitar a continuidade dos serviços instalados e de garantir a alta disponibilidade objetiva.

4.3.6. O Suporte Técnico deverá ser acionável e realizado de segunda a sexta, no horário das 08:00 às 11:30 horas e das 13:30 às 17:00 horas, compreendendo:

- **manutenção corretiva:** série de procedimentos destinados a reparar e a corrigir os componentes dos equipamentos e serviços, sem ônus à Prefeitura de Garibaldi, mantendo seu pleno estado de funcionamento, removendo definitivamente os defeitos eventualmente apresentados;
- **manutenção adaptativa:** série de procedimentos destinados a adequar os itens de configuração em razão de alterações no ambiente tecnológico que suporta os equipamentos e serviços devendo a licitante informar à Prefeitura de Garibaldi a necessidade de atualização de qualquer software relativo à solução de NGFW;
- A sede/filial da licitante deverá estar localizada a no máximo 130 quilômetros do Centro Administrativo da prefeitura, viabilizando o prazo de atendimento presencial;

4.4. IMPLANTAÇÃO

4.4.1. A solução de NGFW atualmente existente no município é do fabricante FORTINET, utilizando o hardware “Fortigate 80F” com firmware na versão 7.4.12, o sistema de auditoria e gestão de relatórios está configurado em ambiente virtual, utilizando a plataforma Hyper-V da Microsoft;

4.4.2. O processo de implantação tem por objetivo a inserção do hardware e software na infraestrutura da PREFEITURA de forma que o resultado final seja uma solução de NGFW com as mesmas características de organização interna (regras de firewall, conexões com AD, interfaceamento, VLANS, etc.) da solução atual;

4.4.3. A PREFEITURA designará um profissional responsável para acompanhamento e fornecimento de todas as informações pertinentes à implantação;

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

4.4.4. Todas as atividades relativas à implantação deverão acontecer em dias úteis (SEGUNDA-SEXTA) no intervalo das 08:00 – 17:00hs, remotamente ou presencialmente, de acordo com a necessidade;

4.4.5. A LICITANTE deverá fornecer um plano de implantação contendo minimamente as etapas e prazos para ser atingidos até a conclusão da implantação e início da prestação do serviço. Este plano deverá ser submetido ao Departamento de T.I do município para avaliação e posterior liberação para início dos trabalhos de implantação;

4.4.5.1. Em caso da solução de NGFW ser do mesmo fabricante da solução atual do município, a LICITANTE poderá substituir o plano de implantação por acesso prévio à nova solução para avaliar a migração direta das configurações através da cópia/restauração do arquivo de configuração;

4.4.6. A solução a ser adquirida deverá ser configurada de maneira que não seja necessário aquisição de novo hardware ou software para o seu pleno funcionamento;

4.4.7. A solução a ser adquirida deverá ser configurada de maneira que não seja necessário alterações estruturais no formato de organização da floresta/domínio do Active Directory pertencente ao município de Garibaldi;

4.4.8. A LICITANTE deverá fornecer credenciais com permissões suficientes para que os técnicos do Município de Garibaldi consigam fazer o gerenciamento COMPLETO da solução, incluindo todas as áreas abrangentes ao funcionamento e layout de conexão, criação e alteração de usuários administradores;

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. O prazo de início será a partir da assinatura do contrato, momento a partir do qual a contratada estará autorizada a realizar a instalação, configuração e ativação dos serviços contratados.

5.2. Deverão ser fornecidos todo hardware e licenças para uso e atualização de todos os componentes de software, vacinas de antivírus/malwares, assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período vigente da locação;

5.3. Para os itens que representem bens materiais, a LICITANTE deverá fornecer produtos novos, sem uso anterior. Por cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento;

5.4. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico. 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;

5.5. Toda solução fornecida deverá estar coberta por danos causados por eventos de força maior, com origem elétrica ou do meio ambiente, devendo ser imediatamente substituído sem custos adicionais ao CONTRATANTE;

5.6. O prazo de entrega e ativação da solução é de 30 (trinta) dias corridos contados da data de emissão da ordem de compra;

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

5.7. A solução deverá ser entregue e configurada na Prefeitura Municipal de Garibaldi, localizada na Rua Júlio de Castilhos, 254, Bairro Centro, Garibaldi/RS.

5.5. OBRIGAÇÕES DA CONTRATADA:

5.5.1. Todas as despesas de transporte, hospedagem, alimentação e hora técnica para viagens à Prefeitura serão por conta da Contratada;

5.5.2. A contratada deverá fornecer treinamento sobre o uso das ferramentas de gestão da solução, bem como, de configuração básica dos equipamentos por ela fornecidos, aos usuários do departamento de T.I da prefeitura de Garibaldi;

5.6. OBRIGAÇÕES DA CONTRATANTE

5.6.1. Prestar à contratada todas as informações e esclarecimentos necessários à execução do objeto, sempre que solicitados;

5.6.2. Designar fiscal do contrato, bem como fornecer as condições necessárias para a adequada execução dos serviços;

5.6.3. Efetuar os pagamentos devidos, nas condições, prazos e valores pactuados, após a comprovação da efetiva prestação dos serviços;

5.6.4. Acompanhar e fiscalizar a execução do contrato, por meio de servidor designado.

6. MODELO DE GESTÃO DO CONTRATO

6.1. A secretaria responsável pelo departamento de informática realizará o monitoramento, acompanhamento e supervisão da empresa licitante.

6.2. Caso ocorram irregularidades ou falhas na execução do objeto, a empresa licitante receberá comunicado por escrito sobre as ocorrências verificadas na execução do objeto, estipulando prazo para que seja substituído, reparado ou corrigido.

6.3. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei n° 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.4. As comunicações entre o órgão e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.5. O órgão poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei n° 14.133, de 2021, art. 117, caput).

6.6.1. O responsável pela fiscalização do contrato será o Servidor Marcelo de Borba, de matrícula 5110, responsável pelo T.I. municipal.

6.6.2. O gestor do contrato será o Secretário Municipal de Inovação e Empreendedorismo, Daniel Deconti, de matrícula 5324.

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

6.7. O prazo de vigência da contratação será de até 12 (doze) meses, a contar da assinatura do contrato, podendo ser prorrogado sucessivamente por meio de Termo Aditivo, até atingir o limite máximo de 10 anos de vigência, nos limites do artigo 107 da Lei 14.133/2021, a critério da Secretaria Contratante.

7. CRITÉRIOS DE RECEBIMENTO E PAGAMENTO

7.1. Caso haja algum serviço em desacordo com as especificações constantes no Termo de Referência e na proposta ou que seja de péssima qualidade, deverão ser reparados no prazo de 15 (quinze) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades. Neste caso, a nota fiscal será retida até que seja regularizada a pendência, sendo autorizado o pagamento após a liberação da pessoa responsável.

7.2. Os pagamentos serão efetuados mensalmente, até o 30º (trigésimo) dia do mês subsequente ao da prestação do serviço, comprovada a execução dos serviços e juntadas as notas fiscais exigidas, conforme calendário de pagamentos a fornecedores.

7.3. A forma de pagamento será por meio de crédito em conta bancária, devendo a contratada informar banco, agência, operação e número da conta bancária em nome da contratada, ou através de boleto de cobrança bancária.

7.4. Quando a cobrança ocorrer por boleto, o mesmo somente poderá ser emitido com código de barra padrão FEBRABAN com vencimento apresentação.

7.5. Os pagamentos ficarão condicionados ao atesto do fiscal do contrato quanto à regular execução dos serviços, bem como à comprovação da manutenção das condições de habilitação e da regularidade fiscal da contratada.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR/PRESTADOR DE SERVIÇO

8.1. A contratação será realizada por meio de licitação, na modalidade Pregão, na sua forma eletrônica, com critério de julgamento por menor preço por lote, nos termos dos artigos 6°, inciso XLI, 17, § 2°, e 34, todos da Lei Federal nº 14.133/2021.

8.2. Para fornecimento/prestação dos serviços pretendidos os eventuais interessados deverão comprovar que atuam em ramo de atividade compatível com o objeto da licitação, bem como apresentar os seguintes documentos a título habilitação, nos termos do art. 62 da Lei Federal nº 14.133/2021:

HABILITAÇÃO JURÍDICA

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

HABILITAÇÃO 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 expedida pela Procuradoria Nacional da Fazenda (Certidão Conjunta de Débitos relativos a Tributos Federais e à Dívida Ativa da União).

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

c) Prova de regularidade com a Fazenda Estadual.

d) Prova de regularidade com a Fazenda Municipal, sendo da sede do Licitante.

e) Prova de regularidade junto ao Fundo de Garantia por tempo de serviço (FGTS).

f) Certidão Negativa de Débitos Trabalhistas (obtida eletronicamente nos sites do TRT-4 e/ou Regional correspondente do licitante ou TST).

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

HABILITAÇÃO ECONÔMICO-FINANCEIRA

a) Certidão negativa de falência ou concordata expedida pelo distribuidor da sede da pessoa jurídica, em prazo não superior a trinta (30) dias da data da apresentação do documento;

QUALIFICAÇÃO TÉCNICA

a) A licitante deverá apresentar um ou mais atestado(s) de Capacidade Técnica, que comprove(m) sua aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis ou iguais ao objeto especificado neste documento;

b) Declaração emitida pela fabricante dos equipamentos e softwares comprovando que é um canal autorizado com nível de certificações “Advanced” e que está apta para comercializar as licenças, garantias e suporte técnico dos produtos do presente termo de referência;

c) A licitante deve comprovar através do vínculo empregatício (CLT) ou ficha de registro, que possui:

- 01 (um) técnico com certificação em modalidade de “especialista em segurança de redes” ou similar, fornecida pelo fabricante da solução de NGFW;

9. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

9.1. Estima-se para a contratação almejada o **valor total de até R$ 110.195,39**

9.2. O levantamento de mercado demonstrou que a solução pretendida é amplamente utilizada por órgãos públicos das esferas federal, estadual e municipal, existindo diversas contratações com características técnicas equivalentes, evidenciando que os preços praticados são compatíveis com os valores de mercado, observando-se o disposto no Decreto Municipal n.º 4.765/2023, nos termos do art. 23, § 1º, da Lei Federal nº 14.133/2021.

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. A despesa decorrente desta solicitação correrá por conta da dotação orçamentária do orçamento em vigor:

ÓRGÃO: 13 - SEC. MUN. DE INOVAÇÃO E EMPREENDEDORISMO
U.O. : 1 - SEC. MUN. DE INOVAÇÃO E EMPREENDEDORISMO
23.691.0094.2084.0000 - MANUTENÇÃO DOS SERVIÇOS DA SMIE
3.3.9.04.00.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – 1340
3.3.9.04.01.30.00.00.00 - COMUNICAÇÃO DE DADOS - 134013

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br

Garibaldi, 30 de julho de 2026.

MARCELO DE BORBA:96069678087
Assinado de forma digital por MARCELO DE BORBA:96069678087
Dados: 2026.08.10 11:18:00 -03'00'

Marcelo de Borba
Assessora de Departamento

DANIEL DECONTI:02111374059
Assinado de forma digital por DANIEL DECONTI:02111374059
Dados: 2026.08.10 15:56:35 -03'00'

Daniel Deconti
Secretário de Inovação e Empreendedorismo

Rua Júlio de Castilhos, 254 – Centro – Garibaldi-RS CEP: 95720-000
Fone: (54) 3462-8200 – www.garibaldi.rs.gov.br