



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

TERMO DE REFERÊNCIA

OBJETO

Contratação de serviços contínuos de empresa especializada no ramo da tecnologia da informação, para prestação de serviços críticos a Prefeitura Municipal de São Gabriel-RS nos termos descritos neste projeto, conforme condições e exigências estabelecidas neste instrumento.

CONDIÇÕES GERAIS DA SOLUÇÃO

A solução visa atender às necessidades atuais e futuras de segurança computacional referentes ao gerenciamento, controle de acesso, garantia de acesso remoto seguro a rede e aos usuários; gestão de incidentes e utilização inteligente de conectividade, elevando o nível de segurança estabelecido na rede corporativa interno, diminuindo a complexidade de gerência do ambiente, assim como aumentando a proteção contra os ataques cibernéticos adotando o modelo de "ZeroTrust" (Confiança Zero) com filtragem e análise do tráfego interno e disponibilização de gerência para administração e consulta de logs centralizada adequando-se às normas internacionais de segurança.

Tendo em vista a necessidade de solução profissional, voltadas para segurança da informação, não será aceito solução OpenSource ou na modalidade Free com customização pela contratada, plataforma WhiteLabel, sendo aceito apenas soluções proprietárias e robusta de mercado.

A participante deverá indicar marca, modelo e endereço (URL) do catálogo da(s) solução(ões) na proposta inicial, para que possa ser validado o pleno atendimento dos requisitos básicos. Deverá indicar todos os módulos, licenças e componentes necessários para formulação da proposta, sob pena de desclassificação.

Todos os bens contratados deverão vir acompanhados de documentação comprobatória do próprio fabricante em relação às características exigidas.

Todas as cláusulas deste termo de referência, bem como todos os itens e subitens das especificações têm caráter obrigatório, e o não cumprimento ou a falsidade no



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

cumprimento de qualquer cláusula ou requisito acarretará a desqualificação do proponente do certame.

A CONTRATANTE terá direito de rejeitar quaisquer componentes da solução que não cumpram todas as exigências deste termo, mesmo após a assinatura de contrato, ficando a CONTRATADA obrigada a adequar, às suas expensas, a solução às cláusulas deste termo de referência no prazo máximo de 20 (vinte) dias úteis a contar do fim da implantação da solução.

FUNDAMENTAÇÃO TÉCNICA – NECESSIDADE DE AMPLIAR SEGURANÇA

A Prefeitura Municipal de São Gabriel/RS, tem necessidade de investir em soluções de segurança de forma imediata, visto que os últimos investimentos em tecnologia foram realizados faz tempo, com a implantação de uma infraestrutura de rede que já se encontra defasada perante as novas ameaças.

Diante disso precisamos atualizar nossas proteções para enfrentar o crescente número de ameaças desenvolvidas diariamente. A título de exemplo apenas a rede federal do governo brasileiro, nos últimos meses já enfrentou mais de 50.000 ameaças, isso quer dizer que são 130 ameaças por dia apenas nas redes monitoradas do governo federal diante dos dados apresentados no CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

Mês	Vulnerabilidades	Incidentes	Total
janeiro	2416	2947	5363
fevereiro	1545	1563	3108
março	1513	2320	3833
abril	2563	2633	5196
maio	2987	2028	5015
junho	2814	1381	4195
julho	3440	1414	4854
agosto	2039	1793	3832
setembro	1696	1948	3644
outubro	1993	2389	4382
novembro	1522	1301	2823
dezembro	1801	1960	3761
Total	26329	23677	50006

Fonte: CTIR Gov



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

Desse modo, esta instituição precisa enfrentar de forma direta tais ameaças digitais, com isso se faz necessário a contratação de empresa especializada no segmento de segurança da informação/tecnologia, que possa prestar serviços de proteção e segurança de nível avançado, uma vez que não temos equipamentos, hardwares, software nem profissionais qualificados para realizar tais atividades, visto que o quadro interno desta prefeitura é reduzido e esta atividade carece de dedicação elevada.

NECESSIDADE/JUSTIFICATIVA COMPLEMENTARES

Sem uma solução de proteção adequada, a prefeitura ficará vulnerável a ataques cibernéticos, como o Ransomware, que podem bloquear computadores e servidores, impedindo parcial ou totalmente o acesso a sistemas essenciais até que um “resgate” seja pago para a liberação dos dados.

Outro exemplo é o ataque de força bruta (Brute Force), que tenta todas as combinações possíveis até descobrir senhas de acesso. Além disso, outros tipos de ameaças podem comprometer a integridade e segurança das informações, colocando em risco os dados da prefeitura e de todos os usuários da rede, conforme já apresentamos dados da rede CTIRGov.

Ressaltamos ainda que a contratação será fundamental para o gerenciamento de permissões e regras da rede e proteção externas. Sem a solução de segurança, não é possível controlar acessos indevidos, como o uso de plataformas de entretenimento (YouTube, Netflix), redes sociais pessoais, sites com conteúdo impróprio e jogos online, que podem comprometer a disponibilidade da internet para os serviços essenciais da Prefeitura Municipal de São Gabriel-RS.

A Prefeitura Municipal de São Gabriel-RS busca contratar um serviço de segurança de rede para fortalecer a proteção dos sistemas, garantir a continuidade das operações e assegurar a confiança da população nos serviços públicos.

Diante do aumento das ameaças cibernéticas e do crescente uso de tecnologias digitais na administração pública, a segurança da rede tornou-se uma prioridade para proteger a integridade dos dados e manter os serviços essenciais em funcionamento.

A principal vantagem da contratação de um serviço especializado é a proteção contra-ataques cibernéticos, reduzindo vulnerabilidades e garantindo um ambiente digital mais seguro. Para isso, a administração pretende adotar uma plataforma de mercado voltada à proteção de ambientes críticos, com total suporte da fabricante e da empresa contratada.

Além disso, a prefeitura deverá ter acesso ao suporte da solução, sempre que necessário, garantindo seus direitos de assistência tanto junto à empresa fornecedora do serviço quanto ao próprio fabricante da solução.



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

A solução ofertada deve ser atual, sem aviso de fim de suporte ou descontinuação por parte do desenvolvedor no momento do pregão. Não serão aceitas soluções em desenvolvimento, customização fase de teste, demonstração, trial ou na modalidade MSP. Materiais necessários para a implementação deverão estar disponíveis e registrados em nome da Prefeitura durante toda a vigência contratual, devidamente vinculados ao fabricante com as respectivas informações.

A Prefeitura Municipal de São Gabriel-RS busca fortalecer sua segurança digital contra diversas ameaças cibernéticas e ataques de negação de serviço (DDoS). Tais ataques, se bem-sucedidos, podem causar danos significativos, incluindo o roubo de dados sensíveis, a paralisação de sistemas e a perda de confiança da população. Para mitigar esses riscos, o serviço de segurança de rede adotará mecanismos avançados de proteção, como sistemas de detecção de intrusões, detectores de ameaças e outras ferramentas especializadas que bloqueiam ataques antes que possam comprometer a infraestrutura municipal, sejam no segmento LAN como no segmento WAN, além de proteger serviços internos e externos, realizando a mitigação e controle de acesso de dados.

A segurança da rede é essencial para a continuidade dos serviços públicos, que abrangem áreas críticas como saúde, educação, finanças e atendimento ao cidadão. A implementação de uma proteção robusta garante que esses sistemas operem de forma estável e segura, mesmo diante de tentativas de invasão.

A proteção de dados é um aspecto crítico para qualquer instituição pública, especialmente no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD). A contratação de um serviço especializado em segurança de rede garantirá que a Prefeitura Municipal de São Gabriel-RS cumpra as exigências legais relacionadas à proteção e ao tratamento adequado dos dados dos cidadãos. Isso inclui a criptografia de informações sensíveis, o controle rigoroso de acessos e a implementação de políticas de privacidade e segurança, prevenindo vazamentos e usos indevidos. A conformidade com a LGPD não apenas evita multas e sanções, mas também reforça a confiança da população nos processos de gestão e proteção de seus dados pessoais, conforme consta na lei.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

Desse modo a própria lei de proteção de dados, apresenta elementos voltadas a necessidade de investimentos em segurança da informação e proteção de dados.



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

REQUISITOS DOS SERVIÇOS– DESCRITIVO DA SOLUÇÃO

SOLUÇÃO DE PROTEÇÃO EM CLOUD

Fornecimento de plataforma em cloud, para gerenciamento de acesso externos, oriundos da internet, com modelo de operação tipo proxy, permitindo criar proteções em camadas a partir de múltiplos conjuntos de regras de W.A.F para aplicativos e acessos HTTPS/HTTP, geridos diretamente cloud da fabricante, reduzindo acessos indevidos diretamente na internet, economizando recursos de processamento, podendo atuar como proxy(ponte) entre recursos na infraestrutura local e recursos alocados em outras clouds.

A plataforma tipo Proteção de aplicação web – W.A.F Cloud;

Segurança provida por meio de API;

A plataforma indicada deverá ser alocada na nuvem da fabricante (cloud) e realizara a sustentação de serviço de segurança. Os recursos devem estar disponíveis mediante a configuração em plataforma própria do desenvolvedor em cloud, a escolha dessa condição visa escolher solução capaz de mitigar e evitar ameaças diretamente na nuvem, de forma que a ameaçaseja retida antes de chegar na infraestrutura local(ip públicos dos serviços), diante disso esse recurso deve obrigatoriamente ser alocado e gerenciado diretamente na nuvem, ademais existem inúmeros fabricantes que operam com soluções desse porte.

A solução deve ter capacidade de operar como distribuição de conteúdo de rede – CDN.

A solução deve oferecer os seguintes serviços em uma única plataforma integrada do fabricante.

Os serviços W-A-F Cloud devem ser prestados mediante uma plataforma web unificada do fabricante e não intrusiva, ou seja, sem a necessidade de instalação de hardware para proteção cloud.

Os serviços contratados deverão monitorar o volume de tráfego ou throughput mensal entregue pela plataforma.

Deverá prover serviço de bloqueio de acessos indevidos, visando evitar que tentativas de ataque em nuvem, desse modo reduzindo os acessos desnecessários.

A plataforma de segurança CDN deverá fornecer o serviço de controle de camada IP para bloqueio ou liberação de endereços IP. Tais listas devem ser propagadas por toda a infraestrutura da Rede de Distribuição de Conteúdo.



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONÔMICO**

A plataforma de segurança CDN deverá possuir capacidade de ocultar os websites e aplicações, restringindo o acesso dos usuários diretamente na origem, fornecendo uma camada adicional de proteção, através de uma lista definida de endereços IPs que têm permissão para se comunicar com a origem da aplicação, podendo controlar via GEO-IP de forma mais eficiente.

A plataforma de segurança CDN deverá suportar a criação de listas de bloqueio ou liberação de sub-redes ou blocos de IPs.

A plataforma de segurança possuir funcionalidade de DNS de pesquisa em nuvem, visando acelerar a resolução de nomes e proteger contra-ataques aos serviços de DNS das consultas públicas efetuadas aos serviços internos da prefeitura, operando de forma proxy WAF.

A plataforma deve ter o seu serviço DNS 100% compatível com DNSSEC, conforme regras do Registro.br para domínios com os sufixos `com.br` ou `rs.gov.br`.

A plataforma deve possuir suporte a zona de pesquisa direta e zona de pesquisa inversa.

Deverá possuir mecanismo ou serviço de detecção, identificação robôs (botnets/bot), de forma a proteger os websites e as aplicações desta Prefeitura, evitando determinado tipos de consultas automatizadas, mediante a regras.

A plataforma deverá possuir caminhos redundantes de acesso e distribuição de conteúdo, a fim de garantir o acesso a seus serviços, bem como ao serviço de origem, a plataforma deverá conter no mínimo 200 pontos de presença ou espelhamento, evitando assim downtimes de serviço.

A plataforma deverá acelerar e distribuir indistintamente quaisquer aplicações baseadas em Protocolo de Transferência de Hipertexto (Hypertext Transfer Protocol, HTTP e HTTPS), balanceando entre seus POPs, a carga das páginas de modo a garantir melhor performance.

A plataforma deve permitir a aceleração utilizando aplicações HTTP/S, usando certificado próprio da plataforma ou certificado da própria instancia do servidor.

Após a configuração dos certificados, deverão ser testados utilizando a ferramenta Qualys SSL Labs (www.ssllabs.com/ssltest), na qual deverá ser obtida a qualificação "A/B" para todas as URLs.

A plataforma deve possuir seus certificados emitidos com certificado raiz da autoridade certificadora dentre as que já vêm previamente instaladas e configuradas nos principais navegadores e dispositivos do mercado suportando, no mínimo: Mozilla Firefox, Google Chrome, Internet Explorer, Safari, iPhone, Android e Windows Phone.



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

A CONTRATADA deverá manter e gerenciar o certificado válido durante todo o período do contrato.

A plataforma deve possuir a capacidade de configuração das cifras e da versão de TLS.

A plataforma deve possuir validação da organização emissora do certificado digital, incluindo os dados do órgão.

A plataforma deve permitir o controle de pelo menos 150 regras básicas.

A plataforma deve TCPturbo.

A plataforma deve ser capaz de identificar falhas, caso haja indisponibilidade em um dos links usados no datacenter de origem, para contínua transmissão e entrega do conteúdo mediante a contratação de licença futura.

A plataforma deve ser compatível com WebSockets.

A plataforma deve proteger, monitorar e emitir alertas de ataques DDoS.

A plataforma CDN deverá possuir os seguintes recursos para a gestão de cache.

A plataforma deve ter suporte a controle de ameaças por Reputação.

A plataforma deverá possuir opção cache analíticos.

A plataforma deverá tratar de maneira individualizada as requisições maliciosas direcionadas aos sites WEB da origem e bloqueá-las.

A plataforma deverá permitir a criação de políticas de cache estáticos, melhorando performance.

A plataforma deverá realizar inspeção completa de corpo de requisições HTML/s, sem limitação de tamanho.

A plataforma deverá disponibilizar em todos os Pontos de Presença o serviço de W.A.F – voltados para proteção de aplicação, visando impedir atividades maliciosas, incluindo pelo menos as seguintes funcionalidades, além de outros tipos de ataques comuns e vulnerabilidades conhecidas a serem bloqueadas a exemplos: Bloqueio por rede e IP, Geolocalização, Secure token, Cross site scripting, Remote file inclusion, Directory transversal e SQL injection.

A plataforma deverá possuir proteção contra as vulnerabilidades WEB, exemplos a seguintes: *Injection, como injeções de SQL, NoSQL, OS e LDAP, Broken Authentication and Session Management, Cross-Site Scripting (XSS), Insecure Direct Object References, Security Misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control;*



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

A plataforma deverá prover serviço de defesa visando mitigar os efeitos de ataques de Distributed Denial-Of-Service (DDoS), sobre o conteúdo distribuído através dos de sua estrutura ou servidores de borda, evitando que estes ataques alcancem a origem dos dados.

A plataforma deverá ser entregue e licenciada para controlar 1(um) domínio sem custos adicionais, permitindo diversos host dentro do mesmo domínio ou subdomínio.

A plataforma deverá mitigar ataques de forma transparente, absorvendo e bloqueando ataques de TCP/IP SYN flood nos seus endereços IP mantendo a disponibilidade do serviço e entrega das aplicações.

A plataforma deverá fornecer o serviço de detecção e mitigação de ameaças para tráfego HTTP e HTTPS. O serviço deve continuar escalável instantaneamente e manter alta performance.

A plataforma deverá absorver e tratar as ameaças WEB na origem do ataque, absorvendo o tráfego malicioso e criando proteção de perímetro dentro da Internet. A plataforma deverá detectar o acesso de robôs nos sites e IP públicos do DNS usados pela Prefeitura.

A plataforma deverá ser entregue e licenciada para controlar no mínimo 15 regras WAF.

A plataforma deverá ser capaz monitorar ou controlar bots específicos sejam definidos como bots amigáveis, exemplo google analíticos.

A plataforma deverá ser capaz de aplicar ações de segurança para os robôs, reduzindo eventuais ameaças digitais.

A plataforma deverá prover solução em nuvem para os serviços de DNS autoritativo.

A plataforma deverá operar com os serviços tipo *DNSSEC (Domain Name System Security Extensions)*.

A plataforma deverá ter ao menos pontos de presença (infraestrutura) no Brasil para melhorar a performance de seus acessos (CDN).

A Plataforma deverá prover mecanismos para eventual aceleração de resolução de nomes DNS;

SOLUÇÃO DE PROTEÇÃO LOCAL

Características Específicas da solução de segurança, voltada para proteção de infraestrutura, interna, obrigatoriamente deverá ser plataforma baseada em hardware, dedicado para processo e controle de segurança da informação, que serão implantados na



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

infraestrutura local, realizado processos de VPN, filtragem de navegação, controle de internet, balanceamento de acesso e demais recursos, indicados no termo.

Performance de processamento para manter a segurança de uma rede interna composta com wifi, switches, computadores e servidores na ordem de até trezentos ativos;

A solução deve possuir proteção de rede com funcionalidades de proteção, e console de gerência, monitoração e logs, bem como possuir demais componentes necessário para proteção de segurança de redes e infraestrutura computacional.

A solução deve possuir funcionalidades de segurança entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões,

A solução deve possuir plataforma capaz de otimizar análise de conteúdo de aplicações em camada sete. Deve ter demais proteções de redes de forma acelerada e otimizada para que o ambiente tenha o mínimo de impacto com a varredura de ameaças;

A solução deve possuir software próprio e customizado para operações de segurança, em versão de mercado, sendo necessário no momento de instalação utilizar-se da versão mais atualizada da solução proposta;

A solução deve possuir uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica, a plataforma a ser utilizada, deverá ser totalmente customizada e voltada para operações de segurança em formato de appliance de mercado, desenvolvido pelo próprio fabricante do software, não sendo aceito computadores ou servidores montados. A participante deverá apresentar comprovação que atende plenamente ao edital, o documento apresentando deve ser emitido pelo desenvolvedor com número do respectivo processo, demonstrando que a proponente está apta para fornecimento da solução e que a solução atende plenamente todos os recursos técnicos previstos.

A atualização de software deverá enviar avisos de atualização automáticos;

A solução possuir sistema de objetos, permitindo a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores,

A solução deve permitir o backup das conf diariamente, com a opção de escolher o local de armazenamento;

A solução ter suporte SNMPv3 e Netflow/Sflow;

A solução deverá ser statefull, com inspeção profunda de pacotes (deep packet inspection);

A solução deve permitir ser dividida pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis;



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

A solução deve permitir as políticas de NAT deverão ser customizáveis para cada regra;

A solução deve ter proteção contra flood deverá ter proteção contra DoS (Denial of Service), DDoS (DistributedDoS) e bloqueio de portscan;

A solução ter proteção contra anti-spoofing;

A solução possa suportar IPv4 e IPv6;

A solução deve suportar IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969;

A solução deve ter suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPFv3) e multicast (PIM-SM e IGMP);

A solução deve suportar a definição de VLANs conforme padrão IEEE 802.1q e tagging de VLAN;

A solução deve permitir balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso;

A solução deverá permitir armazenamento interno (SSD/M2) mínimo de sessenta gigabytes.

A solução deverá permitir port-aggregation de interfaces suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

A solução deve ser constituída hardware com no mínimo duas portas UBS;

A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP;

A solução deve permitir o trafficshapping (QoS) deverá ser baseado em rede ou usuário;

A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas;

A solução deve possuir homologação/certificação FIPS-140-2;

A solução deverá ser entregue, instalada configurada e ajustada para operar em HA (redundância) física, no qual deverá ser constituída por 2 unidades iguais conectadas, fazendo um espelho de configurações, a unidade secundária deverá ter condições de assumir imediatamente os serviços da primária, em caso de falha física do hardware, passando a operar de forma transparente sem intervenção humana para realizar esta operação.

A solução deve possuir otimização em tempo real de voz sobre IP;



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

A solução deve implementar o protocolo de negociação Link AggregationControlProtocol (LACP).

A solução deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários;

A solução permitir o controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas;

A solução deve permitir gestão de políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços;

A solução deve possuir modulo de obtenção de IP maliciosos de forma dinâmica, efetuando bloqueio de endereços com base em lista pré-definidas, que podem ser configuradas na condição de monitoramento ou bloqueio;

A solução deve ter controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

A solução deve possuir homologação/certificação Anatel;

A solução deve permitir controle de políticas por países via localização por IP;

A solução deve permitir suporte a objetos e regras IPV6;

A solução deve permitir suporte a objetos e regras multicast.

A solução deve ser capaz de realizar proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Anti-Malware e Proteção Web de servidores integrados;

A solução deve realizar a inspeção profunda de pacotes (DPI deeppacketinspection) para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS);

A solução ter suas assinaturas de prevenção de intrusão (IPS) devem ser customizadas;

A solução deve permitir exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;

A solução deve suportar granularidade nas políticas de IPSe Anti-Malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;

A solução deve ter a proteção Anti-Malware deverá bloquear todas as formas de ameaças, web malwares, trojans e spyware em HTTP e HTTPS e FTP;



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

A solução deve realizar a proteção Anti-Malware deverá realizar a proteção com emulação JavaScript;

A solução deve no mínimo seis interfaces de redes em velocidade mínima de um Gigabyte por segundo RJ-45;

A solução deve ter proteção em tempo real contra novas ameaças criadas;

A solução deve possuir engine interna para a detecção de malware;

A solução deve permitir o bloqueio de vulnerabilidades;

A solução deve possuir dois conectores de fonte de alimentação;

A solução deve permitir o bloqueio de exploits conhecidos;

A solução deve detectar e bloquear o tráfego de rede que busque acesso a contactcommand e servidores de controle utilizando múltiplas camadas de DNS;

A solução deve detectar e bloquear o tráfego de rede de forma preventiva utilizando-se do protocolo de consulta DNS, para tanto a solução deverá disponibilizar o próprio DNS, no qual deve possuir diversos critérios a redução de ameaças com base no controle das consultas DNS efetuadas, gerando inclusive relatórios e gráficos de tais consultas.

A solução deve incluir proteção contra-ataques de negação de serviços;

A solução deve ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP Flood, etc.

A solução deve possuir avaliação pelo Gartner Customers' Choice 2024 (ou mais recente) com pontuação mínima de 4.6;

A solução deve no mínimo duas interfaces de redes em velocidade mínima de um Gigabyte por segundo SFP;

A solução deve suportar bloqueio de arquivos por tipo;

A solução deve ser capaz de registrar no console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

A solução deve reportar os eventos devem identificar o país de onde partiu a ameaça;

A solução deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

segurança, etc, ou seja, cada política e poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança;

A solução deve realizar proteção de aplicação Web deverá ter a função de reverse proxy, com a função de URL hardening realizando deep-linking e prevenção dos ataques de path traversal ou directorytraversal;

A solução deve realizar proteção de aplicação Web deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de performance da proteção e permissão e bloqueio de ranges de IP;

A solução deve realizar proteção de ameaças com proteção da aplicação Web;

A solução deve realizar proteção contra os seguintes ataques, mas não limitado a: SQL injection e Cross-site scripting.

A solução deve controlar dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, porthopping e túnel através de tráfego SSL encriptado;

A solução deve reconhecer aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web-email e update de softwares;

A solução deve reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freetag Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewerConferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web. Tal função dentro da solução deverá ser capaz de reconhecer no mínimo três mil aplicativos diferentes;

A solução deve realizar proteção de ameaças com proteção real time sendo capaz de processar quatro gigabyte por segundo para ThreatProtection;

A solução deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin,



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freerate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIn (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website);

A solução deve realizar o escaneamento de micro app deverá ser habilitado via console gráfica (GUI) e via comando de linha (CLI);

A solução deve controlar o tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

A solução deve ser capaz de operar com no mínimo seis milhões de conexões simultâneas;

A solução deve atualizar a base de assinaturas de aplicações automaticamente;

A solução deve reconhecer aplicações em IPv6;

A solução deve limitar a banda usada por aplicações (trafficshaping);

A solução deve operar como dispositivos de proteção de rede, possuindo a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

A solução deve permitir adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

A solução deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuem acesso a estes aplicativos devem ter a utilização bloqueada.

A solução deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez;

A solução deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

A solução deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Radius, E-directory e base de dados local;

A solução deve popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

A solução deve possuir categorias de URLs já padronizadas (no mínimo noventa tipos distintos de categorias) e permitir que sejam criadas categorias customizadas;

A solução deve suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

A solução deve ser capaz de forçar o uso da opção Safe Search em sites de busca;

A solução deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;

A solução deve suportar a criação categorias de URLs customizadas;

A solução deve suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

A solução deve permitir a customização de página de bloqueio;

A solução deve suportar a inclusão nos logs do produto de informações das atividades dos usuários;

A solução deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado;

A solução deve realizar caching do conteúdo web;

A solução deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

A solução deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, Active Directory, Radius, eDirectory, Azure, TACACS+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONÔMICO**

A solução deve permitir o controle, sem instalação de cliente de software, que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente na solução (Captive Portal);

A solução deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

A solução deverá ter proteção contra ameaças de servidores, com recurso W.A.F integrado.

A solução deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64;

A solução deve possuir a autenticação com plataformas tipo Azure, MS Active Directory e eDirectory;

A solução deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

A solução deve controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações;

A solução deverá suportar TrafficShaping (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD;

A solução deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado;

A solução deve suportar priorização Real-Time de protocolos de voz (VoIP).

A solução deve suportar VPN Site-to-Site e Cliente-to-Site;

A solução deve suportar IPsec VPN;

A solução deve suportar SSL VPN;

A solução deve suportar L2TP e PPTP;

A solução deve suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD;



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

A solução deve ser disponibilizada o acesso remoto ilimitado, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL para estações Windows, caso necessário licenciamento, este recurso deve ser entregue licenciado para pelo menos quinhentas conexões de VPN;

A solução deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows;

A solução deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, HTTP, HTTPS, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso;

A solução deve permitir VPN IPsec e suportar: DES e 3DES, Autenticação MD5 e SHA-1; Diffie-Hellman Group 1 e Group 14;

A solução deve permitir criar políticas de controle de aplicações, IPS, Anti-Malware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

A solução deve suportar autenticação via AD/LDAP, Token e base de usuários local;

A solução deve permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, Active Directory, Radius, eDirectory, TACACS+ e via base de dados local.

A solução deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversas unidades através de uma única console central, com administração de privilégios e funções;

A solução deve ter o gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar na plataforma de segurança;

A solução deve estar licenciada completa, com todos os recursos informados, durante a vigência contratual;

A solução deverá ter compatibilidade FIPS-140;

A solução deve possuir plataforma centralizada a gerência de políticas e configurações para as soluções de segurança, sem necessidade de acesso direto via IP;

A solução deve possuir gerenciamento da solução deve suportar a interface de administração via navegador (browser);

A solução deve ter interface de gerenciamento deverá ser preferencialmente no idioma português Brasil, podendo ser em inglês;



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

A solução deve permitir a retenção de eventos e logs diretamente na nuvem, com capacidade de coletar no mínimo duzentos gigabytes de armazenamento, durante a vigência contratual, além do armazenamento interno na própria unidade;

A solução deve permitir a criação de templates para configurações;

A solução deve possuir indicadores do estado de externamente com indicado do status rede;

A solução deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de digitais, navegação, entre outros;

A solução deve permitir a criação de grupos por nome, modelo, firmware e regiões;

A solução deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);

A solução deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de rollback de configurações para mudanças indesejadas, na plataforma de gestão em nuvem deverá ser capaz de efetuar a retenção de pelo menos 5 configurações/backup;

A solução deve ter logs de auditoria de uso administrativo e atividades realizadas na solução;

A solução deve ter integração nativa com a solução de logs e relatórios, habilitando o provisionamento automático de novos dispositivos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios, sem custo adicional para a CONTRATANTE.

A solução deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central;

A solução deve prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando;

A proponente deverá apresentar, no mínimo, um profissional que será designado para os serviços técnico, para tanto é necessário apresentar certificação emitida pelo desenvolvedor da solução de proteção hardware(appliance) ofertada.

A solução deve ter a possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda;



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

A solução deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, webserver e demais ameaças;

A solução deve fornecer relatórios históricos para análises de mudanças e comportamentos;

A solução deve conter customizações dos relatórios para inserção de logotipos próprios;

A solução deve permitir a exportação via PDF ou Excel;

A solução deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia;

A solução deve fornecer relatórios de tendências de ameaças;

A solução deve fornecer logs em tempo real, de auditoria e arquivados;

A solução deve possuir mecanismo de procura de logs arquivados;

A solução deve ter acesso baseado em Web com controles administrativos distintos.

CONDIÇÕES DE EXECUÇÃO

A contratada deverá fornecer todos os serviços, conforme indicados na tabela de preços, para itens da proposta, será realizada a contratação imediatamente após o envio do contrato, porém no caso das horas técnicas, será acionada conforme demanda técnica ou operacional que possam surgir ao longo do contrato.

DO SERVIÇO DE INSTALAÇÃO DA SOLUÇÃO - SETUP INICIAL

Para a solução descrita neste termo, a contratada deverá efetuar a instalação, configuração e customização inicial dos serviços disponibilizado pela Prefeitura;

A instalação deverá ser realizada por técnicos treinados da própria contratada, e ocorrerão em horários a serem combinados com o Departamento de Informática da Prefeitura, de forma a evitar que prejudique as atividades normais das repartições públicas municipais;

Toda a despesa de deslocamento, hospedagem e refeição deve ser de responsabilidade da contratada, sendo considerada todas as atividades de instalação de forma PRESENCIAL.

Os serviços deverão ser implementados, configurados e ativados pela CONTRATADA nos locais indicados no termo.



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONÔMICO**

Os serviços de instalação e configuração da solução devem ser executados nos seguintes endereços: Sede da Prefeitura Municipal de São Gabriel-RS.

A instalação deverá ser previamente agendada com o gestor do contrato e deverá acontecer em dias úteis no horário a ser combinado.

A CONTRATADA deverá realizar os serviços de instalação e configuração de forma a garantir o seu pleno funcionamento no ambiente tecnológico.

O planejamento, instalação, configuração e ativação deverão ser executados por profissionais qualificados e a empresa deverá ser credenciada pelos desenvolvedores da solução.

A CONTRATADA deverá garantir a implantação de componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução entregue.

Todas as configurações serão realizadas em conformidade com a recomendação do mercado e alinhados com as boas práticas de segurança da informação, bem como os requisitos técnicos indicados pela Prefeitura no ambiente em questão e suas peculiaridades.

Ademais a contratada deverá realizar adaptações e atualizações de parâmetros caso necessário com acompanhamento técnico da contratante.

Os serviços serão instalados, configurados, testados e integrados na estrutura existente (rede de dados) da Prefeitura, garantindo assim a total compatibilidade e interoperabilidade de sua infraestrutura, como no ambiente atual, para proteção de computadores já existe solução vigente e operacional, se faz necessário que a plataforma de proteção local, seja totalmente integrada e compatível com solução da Sophos visto que esse fabricante já tem soluções em nosso ambiente computacional.

O presente processo de contratação será conduzido visando a contratação de solução de segurança. A indicação de fabricante, marcas e modelos como referência técnica para escolha de solução, objetivando integração máxima, essas exigências técnicas e operacionais, encontradas no processo seguem a conformidade com os dispositivos da Lei Federal nº 14.133/2021, que rege os processos de licitação e contratação pública, inclusive no âmbito de bens e serviços de tecnologia da informação e comunicação.

Nos termos do art. 42, § 4º da Lei Federal nº 14.133/2021, **admite-se a indicação de marca de forma excepcional, desde que devidamente justificada por razões de ordem técnica**. Essa medida visa garantir a compatibilidade, o desempenho e a plena adequação dos bens às necessidades específicas da Administração, resguardando, simultaneamente, os princípios da impessoalidade, da eficiência e da competitividade.

Ainda com base nesta justificativa técnica, a Prefeitura Municipal de São Gabriel precisa manter de forma ininterrupta e crítica o atendimento à população, sendo responsável por decisões rápidas e precisas que envolvem a mobilização de recursos de



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

educação, saúde e atendimento interno. Diante disso, a aquisição e substituição de equipamentos de TIC devem obedecer a critérios rigorosos de qualidade, desempenho, segurança e confiabilidade e manter minimamente critérios de compatibilidade.

A indicação de marcas e modelos como referência técnica visa garantir que as contratações possam atender plenamente objetivos de integração, padronização, redução do tempo de implantação.

Ademais a eficiência e Confiabilidade no Atendimento, tendo em vista a natureza do serviço exige equipamentos com alto desempenho, baixa latência, rápida inicialização e elevada disponibilidade, para garantir a continuidade das operações em tempo real, sem falhas ou interrupções que possam comprometer o atendimento à urgência e emergência.

Ademais a condução de processo de compra, também deve ser conduzido visando a padronização Tecnológica e Integração com Sistemas Existentes: A compatibilidade com os sistemas já implantados (solução de proteção para computadores-endpoint), bem como a padronização de equipamentos e configurações, é essencial para assegurar a interoperabilidade e a manutenção dos fluxos operacionais. A adoção de modelos tecnicamente referenciados reduz a complexidade na gestão de ativos e no suporte técnico, desse modo está totalmente justificado a condução de certame visando a contratação de solução com integração total e nativa com as soluções já existentes, conforme indicado claramente na Art. 41. No caso de licitação que envolva o fornecimento de bens, a Administração poderá excepcionalmente: I - indicar uma ou mais marcas ou modelos, desde que formalmente justificado.

PRAZO, LOCAL E HORÁRIOS PARA A PRESTAÇÃO DOS SERVIÇOS

O prazo para a instalação da solução descritos no Termo de Referência para que estejam em pleno funcionamento, **será de 10 (dez) dias corridos**, após a assinatura do contrato, tendo em vista a urgência do sistema e sua devida implementação, podendo o prazo ser prorrogado por igual período desde que justificado pela contratada.

Os serviços de instalação da solução tecnológica deverão ser realizados na sede, localizada na R. Duque de Caxias, 268 - Centro, São Gabriel - RS, 97300-000, em horário de expediente, de segunda a sexta-feira, excetos feriados e ponto facultativo, das 8h00 às 14:00, podendo ser agendando em horário fora do expediente para redução de impactos e danos ao ambiente computacional;

Caso seja necessário data e horário que não sejam dentro do expediente, será programado com antecedência com o gestor do contrato.

Toda prestação de serviço será feita de forma presencial, inclusive suporte, integração e instalação.



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONÔMICO**

VIGÊNCIA CONTRATUAL

Eventuais reajustes serão efetuados apenas naqueles itens com características de serviço contínuo, considerados índices de inflação convencionais como IGMP, SELIC, IPCA entre outros.

Sobre a vigência contratual, fica estabelecido prazo inicial de 24 meses, pode ser prorrogada conforme previsto em lei até o prazo de 10 anos.

RESPONSABILIDADE TÉCNICA

Após a assinatura do contrato, a contratada deverá apresentar a Prefeitura Municipal de São Gabriel/RS a Anotação de responsabilidade técnica- ART referente ao indicado neste termo. Os serviços deverão ser acompanhados pelo responsável técnico da licitante, devidamente registrado no conselho de classe.

APRESENTAÇÃO DE AMOSTRA

A licitante classificada em primeiro lugar poderá ser convocada a apresentar uma amostra física da solução para validação técnica, caso o catálogo anexado ou consultas a fontes públicas sejam insuficientes para comprovar o atendimento ao Termo de Referência. Uma vez solicitada, a solução deve ser instalada presencialmente na sede da Prefeitura em até 10 (dez) dias úteis. Após a avaliação, será emitido um laudo técnico detalhado atestando a conformidade do item.

DA QUALIFICAÇÃO TÉCNICA

A empresa participante deverá apresentar os seguintes documentos:

No mínimo um atestado emitido por pessoa jurídica de Direito Público ou Privado comprovando que já prestou serviços iguais ou superiores a presentes no respectivo termo, por no mínimo 01 (um) ano. Deve ser incluso treinamento, suporte e instalação de solução igual ou superior.

A proponente deverá apresentar um responsável técnico do seu quadro profissional na condição de Engenheiro da Computação, Engenheiro Elétrico ou Engenheiro da Telecomunicações, perante o conselho de classe do endereço de sua sede, acompanhando da sua certidão PJ válida, do respectivo conselho, indicado o profissional vinculado, conforme preconiza a Resolução Interna Anatel nº 428, de 28 de abril de 2025.

A proponente deverá garantir seguir o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (Resolução nº 740, de 21 de dezembro de 2020). Apresentação de cópia da Licença para Prestação do Serviço de Comunicação Multimídia



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

(SCM), emitida pela Agência Nacional de Telecomunicações (ANATEL), devidamente válida e ativa, em nome e no CNPJ da própria Licitante.

É vedada, sob pena de inabilitação, a apresentação de licenças de terceiros, consórcios ou empresas que não participem diretamente do certame, conforme Resolução ANATEL n.º 614/2013, Art. 1º.

DateProtection Officer (DPO) Nomeação e indicação obrigatória de um Data Protection Officer (DPO) ou Encarregado pelo Tratamento de Dados Pessoais, em estrito cumprimento ao Art. 41 da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).

A Licitante deverá apresentar os dados completos do DPO (Nome, CPF, contato) e a documentação comprobatória de seu vínculo formal com a empresa (CTPS, Contrato de Prestação de Serviços ou equivalente).

A ausência da nomeação do DPO, considerando a criticidade dos dados tratados, acarretará a inabilitação imediata da Licitante.

A proponente deverá comprovar as exigências previstas no edital, na documentação da habilitação sob pena de desclassificação, será necessário apresentar prova a vínculo dos profissionais indicados, sendo aceito: CLT, Contrato social PJ, e via certidão PJ do conselho de classe.

HANDS-ON TREINAMENTO

A contratada deverá ministrar treinamento relativo à operacionalização, manuseio, configuração e utilização da solução, visando garantir a transferência de conhecimento para até 3 (três) funcionários indicados pela contratante;

O conteúdo programático da capacitação deverá prever todas as funções necessárias para a correta operação dos serviços previstos por parte dos usuários.

As datas e horários para a realização dos treinamentos serão definidos pela contratante em comum acordo com a contratada;

A contratada será responsável por especificar o ambiente necessário à capacitação, prover o material de acompanhamento do conteúdo das ferramentas de gestão.

Imperioso que seja presencial, na sede da Prefeitura Municipal de São Gabriel-RS, ficando a contratante responsável pela sala, recursos audiovisuais e estações de trabalho que se fizerem necessários à capacitação dos representantes a serem capacitados;



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

Todas as despesas envolvendo treinamento, viagem, deslocamento, alimentação e hospedagem do(s) instrutor(es), correrão por conta da proponente.

ACIONAMENTO TÉCNICO

A contratada deverá realizar atendimento PRESENCIAL, na sede desta prefeitura, quando da necessidade e ajustes nos sistemas de segurança por ela implantados com suporte total.

O atendimento obrigatoriamente deverá ser realizado profissional minimamente qualificado em Engenharia ou Segurança da informação, conforme indicado em Habilitação técnica deste documento;

O(s) profissional(ais) devem obrigatoriamente atender de forma presencial, caso necessário demandas de ajustes, reuniões de alinhamento e melhorias da rede.

Caso seja necessário reinstalação em razão das mudanças internas, ajustes não programados ou não estabelecidos na instalação inicial, será considerado dentro do suporte mensal pagos a contratada.

O acionamento técnico poderá ser utilizado para revisão do ambiente nos segmentos da tecnologia da informação e redes de computadores que se conectam a referida solução implantada.

A atividade técnica de avaliação de segurança desempenha um papel fundamental na segurança cibernética, simulando ataques reais para reforçar as defesas organizacionais. Importante salientar que tal atividade requer conhecimento avançado de redes, sistemas operacionais, aplicações web, engenharia reversa e estratégias ofensivas, sempre com foco na proteção e mitigação de riscos, conforme profissional já estabelecido neste documento, desse modo após implantação se faz necessário revisão de ameaças.

A contratada deverá fazer a migração do DNS e demais proteção em cloud, com proteções máximas ativadas, com foco em redução de ameaças, incluindo recurso de DNSSec.

SUPORTE TÉCNICO PRESENCIAL E REMOTO

NÚMERO DE SOLICITAÇÕES DE ATENDIMENTO: Ilimitado
ABERTURA DE CHAMADOS: POR QUALQUER UM DOS SEGUINTE CANAIS DE ATENDIMENTO: INTERFACE WEB, TELEFONE, 0800 OU NÚMERO LOCAL OU POR E-MAIL.
A PREFEITURA TEM LIBERDADE DE ACIONAR DE FORMA PRESENCIAL 1 VEZ



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

POR MÊS A CONTRATADA PARA AJUSTES, ATUALIZAÇÕES E CORREÇÕES DOS SISTEMAS DE FORMA PRESENCIAL AO LONGO DO CONTRATO, SEMPRE QUE FOR NECESSÁRIO, SEM CUSTOS ADICIONAIS NO CONTRATO.

MODO ATENDIMENTO: IN LOCO PRESENCIAL, ACESSO REMOTO

PRIORIDADE:	BAIXA	NORMAL	URGENTE
SEVERIDADE:	Obstáculo no trabalho de usuários individuais e/ou uma solução aceitável está disponível. O cliente não precisa de solução imediata.	Interrupção do trabalho de usuários individuais e nenhuma solução aceitável está disponível. O cliente não precisa de solução imediata.	Interrupção dos processos críticos, diversos usuários interrompidos de executar seu trabalho e nenhuma solução está disponível. O cliente precisa de uma solução imediata.
SLA INÍCIO: (Prazo de atendimento)	60 MINUTOS	60 MINUTOS	60 MINUTOS
SLA TÉRMINO: (Prazo de resolução)	12 HORAS	8 HORAS	6 HORAS

No caso de suporte técnico seja presencial, sempre deve-se considerar o endereço da Prefeitura Municipal de São Gabriel/RS, no expediente de segunda-feira à sexta-feira, estabelecido ou em horário estabelecido com o setor de Informática para acordar o dia e horário para o atendimento do suporte técnico.

MODELO DE PROPOSTA

A Prefeitura Municipal de São Gabriel-RS

Objeto: Prestação de serviço continuada de tecnologia da informação com fornecimento de insumos, componentes e demais softwares, incluídos suporte durante a vigência contratual.



PREFEITURA DE SÃO GABRIEL
Palácio Plácido de Castro
**SECRETARIA MUNICIPAL DE PLANEJAMENTO, GESTÃO E
DESENVOLVIMENTO ECONOMICO**

Lote 1	item	Descrição dos serviços	Tipo	Prestação mensal	Valor total (24 meses)
1	1.1	Prestação de serviço continuada de tecnologia da informação com fornecimento de insumos, componentes e demais softwares. Suporte durante a vigência contratual.	24 meses	R\$	R\$

No valor mensal deverá estar incluído, todos custos, impostos e deslocamentos necessários.

Em papel timbrado da empresa, com dados, conta bancária, CNPJ e indicação de impostos.

São Gabriel, 23 de Março de 2026.

Anderson S. Bitencourt
Coordenador de Informática