TERMO DE REFERÊNCIA (TR)

Prefeitura Municipal de Lajeado/RS

CAPÍTULO I

DA DEFINIÇÃO DO OBJETO

1. OBJETO

1.1. O presente Termo de Referência tem por objeto disciplinar a contratação de solução integrada de segurança cibernética em modalidade SECaaS (*Security as a Service*), contemplando: fornecimento em regime de locação/aluguel de 01 (um) *appliance* de *Firewall* do tipo *Next Generation Firewall* (NGFW), licenciamento e proteção de, no mínimo, 1.600 (mil e quinhentos) endpoints (incluindo 10 (dez) servidores como endpoints), serviços de implantação, configuração, migração/adequação, operação assistida, suporte técnico especializado, monitoramento SOC (*Security Operation Center* - Centro de Operação de Segurança) 24x7x365, *hardening* contínuo, treinamento para equipe interna e realização de 2 *Pentests*, pelo prazo contratual definido neste TR.

1.2. Para fins de padronização e julgamento, o objeto será estruturado nos itens abaixo:

Especificação do item que compõem o objeto da contratação

Lote único				
Descrição	**Uidade**	Valor mensal	Total anual	Total em 60 meses
Solução integrada de segurança cibernética em modalidade SECaaS (Segurança como serviço - *Security as a Service*)	mês	R$ 38.640,00	R$ 463.680,00	R$ 2.318.400,00

Detalhamento do Objeto para composição do valor do serviço

Item	Descrição	Unidade	Quantidade
1	*Appliance* NGFW (*rack-mount*) com licenças/assinaturas e suporte	un	1
2	Licenciamento e proteção de *endpoints* (estações de trabalho e notebooks) - Antivírus	lic	1.600
3	Licenciamento e proteção de *endpoints* (servidores) incluídos no quantitativo total	lic	10
4	Serviços SECaaS: implantação, operação assistida, suporte, SOC 24x7x365, *hardening* e treinamento	sv	1
5	*Pentest* do firewall e serviços publicados na WEB	sv	2

2. VIGÊNCIA

2.1. Este Termo de Referência tem validade de 60 (sessenta) meses, contados a partir da assinatura do contrato, podendo ser prorrogado em conformidade com o art. 107, da Lei nº 14.133/2021, mediante justificativa da necessidade e vantajosidade para a Administração, com comprovação de preços e condições mais vantajosas.

3. CLASSIFICAÇÃO DO BEM OU SERVIÇO

3.1. O objeto deste Termo de Referência caracteriza-se como bem e/ou serviço comum, pois seus padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado, métricas de capacidade (*throughput*), funcionalidades técnicas e Acordo de Nível de Serviço (SLA), permitindo julgamento por menor preço, sem prejuízo da verificação de conformidade técnica.

CAPÍTULO II

DA FUNDAMENTAÇÃO, DESCRIÇÃO E REQUISITOS

4. DESCRIÇÃO DA NECESSIDADE

A contratação na modalidade SECaaS não representa apenas a aquisição de software ou hardware, mas a incorporação de uma capacidade contínua de defesa cibernética. Esta abordagem é a única capaz de atender, de forma simultânea e sustentável, aos requisitos legais da **LGPD** e às melhores práticas internacionais (**ISO, NIST, CIS e OWASP**), garantindo a continuidade do negócio e a proteção dos ativos de informação da instituição. Deve-se manter conformidade com as leis e normas da área de segurança de TI, conforme apresentado no quadro abaixo.

Quadro de Conformidade Normativa

Item	Descrição do Requisito Técnico	Norma/Lei de Referência
1	**Inspeção de Tráfego Criptografado:** Capacidade de descriptografar e inspecionar tráfego SSL/TLS (versão 1.2 e 1.3) para evitar vazamento de dados pessoais.	LGPD (Art. 46); RFCs de SSL/TLS
2	**Proteção Avançada (NGFW/IPS):** Prevenção de intrusão baseada em assinaturas e comportamento para bloquear ataques conhecidos e *Zero-day*.	ISO/IEC 27002 (Controle 8.15); NIST SP 800-115
3	**VPN com Autenticação Forte:** Suporte a túneis IPsec/SSL VPN com integração a MFA (Múltiplo Fator de Autenticação).	ISO/IEC 2702 (Controle 5.14); RFCs IPsec
4	**Antivírus de Próxima Geração (NGAV):** Detecção de malware por análise heurística e comportamental, além de assinaturas tradicionais.	CIS *Control* 10; ISO/IEC 27002 (Controle 8.7)
5	**Prevenção de *Exploit* em Aplicações:** Proteção contra vetores de ataque listados no Top 10 OWASP (SQLi, XSS, etc.) via filtros de segurança.	OWASP *Testing Guide*; NIST SP 800-115

6	**Gestão e Retenção de Logs:** Armazenamento centralizado de logs de eventos de segurança para fins de auditoria e resposta a incidentes.	ISO/IEC 27035; NIST SP 800-61
7	**Monitoramento e Alertas 24x7:** Sistema de notificação automatizada em caso de detecção de ameaças críticas.	ISO/IEC 27035; NIST SP 800-61
8	***Hardening* de Dispositivos:** Aplicação de configurações de segurança recomendadas para reduzir a superfície de ataque do *firewall/endpoint*.	CIS Controls; ISO/IEC 27001 (SGSI)
9	**Análise de Risco Integrada:** Fornecimento de relatórios periódicos de postura de segurança e riscos detectados no ambiente.	ISO/IEC 27005 (Gestão de Riscos)
10	**Atualização Automática (SECaaS):** Garantia de atualização de *firmware* e bases de ameaças sem intervenção manual ou custo adicional.	ISO/IEC 27002 (Controle 8.8)

4.1. A contratação visa assegurar a continuidade e o aprimoramento da segurança da informação e da cibersegurança no âmbito da Prefeitura Municipal de Lajeado/RS, em especial na proteção do perímetro (borda), estações de trabalho e servidores (*endpoints*), bem como na detecção e resposta a incidentes por meio de monitoramento especializado (SOC). Trata-se de necessidade diretamente relacionada à preservação dos princípios de Confidencialidade, Integridade e Disponibilidade (CID) dos ativos e serviços públicos digitais, reduzindo riscos de indisponibilidade, vazamento de dados, *ransomware* e outras ameaças cibernéticas.

4.2. A evolução do cenário de ameaças, o aumento de exposição de serviços (integrações, acessos remotos, tráfego criptografado e aplicações em nuvem) e a necessidade de respostas rápidas exigem solução integrada, com capacidade de inspeção em camada 7, prevenção de intrusões, filtragem de conteúdo e correlação de eventos. Além da camada tecnológica, a administração necessita de capacidade operacional contínua para manutenção de políticas, resposta proativa, *hardening* e melhoria progressiva da postura de segurança.

4.3. A necessidade pública também decorre da obrigação de garantir conformidade com boas práticas de governança e segurança, incluindo requisitos de sigilo, rastreabilidade, evidências e auditoria. A contratação em modelo SECaaS é orientada à eficiência operacional, pela centralização do ciclo completo: fornecimento/gestão de licenças e assinaturas, manutenção evolutiva e corretiva, suporte 24x7, monitoramento e serviços especializados, reduzindo a dependência de esforços internos para tarefas críticas e garantindo disponibilidade de especialistas.

4.4. O escopo demanda solução dimensionada para o cenário atual e crescimento, contemplando 1.610 *endpoints* (incluindo 10 servidores), com visibilidade centralizada e ações coordenadas entre *firewall* e *endpoint*, além de SOC em regime 24x7x365, com SLA formal. A necessidade é permanente/contínua durante a vigência, pois a proteção deve ser ininterrupta e a resposta a incidentes deve ocorrer dentro de prazos compatíveis com a manutenibilidade e disponibilidade dos serviços públicos.

5. DESCRIÇÃO DA SOLUÇÃO

5.1. A solução SECaaS deverá integrar, no mínimo, três camadas: (i) segurança de borda com NGFW; (ii) segurança de *endpoints* (*antimalware/endpoint security*) com gerência centralizada; (iii) monitoramento e resposta a incidentes (SOC) com *hardening* contínuo e manutenção de políticas. O contratado deverá prover os componentes, licenças, assinaturas, implantação e operação assistida, com suporte especializado 24x7 e com mecanismos de mensuração e evidências de conformidade.

5.2. Componente 1 - NGFW (*Firewall* de Próxima Geração) - *Appliance* (01 unidade)

5.2.1. O equipamento deverá ser do tipo *appliance* NGFW, *rack-mount*, compatível com *rack* padrão 19", com altura máxima de 1U, fornecido com suportes/trilhos e acessórios para fixação. Não serão aceitas soluções baseadas em computadores de uso geral (PC) ou combinações de hardware e software de fabricantes distintos não integrados para a finalidade de NGFW.

5.2.2. O appliance deverá possuir arquitetura voltada à inspeção de conteúdo em camada 7, com reconhecimento de aplicações, identificação de usuários, filtragem de URL, prevenção de ameaças e prevenção a ataques *zero-day*, incluindo, de forma integrada, módulos de IPS, antivírus de borda e *antispyware*.

5.2.3. Capacidades mínimas (requisitos de desempenho e escala), com comprovação por documentação pública do fabricante (*datasheet*):

a) *Throughput* com políticas básicas (L3/L4): compatível com o cenário de tráfego da contratante, devendo ser dimensionado para operação *inline* com margem de crescimento;
b) Inspeção de ameaças (*Threat Prevention*/IPS) e inspeção SSL/TLS com desempenho compatível com o uso institucional;
c) Capacidade de sessões simultâneas e de novas conexões por segundo compatível com ambiente corporativo multiusuário;
d) Suporte a VPN IPsec e SSL VPN, com licenciamento adequado ao ambiente, permitindo expansão sem troca do equipamento;
e) Armazenamento local para *logs* e evidências, com retenção e exportação, e possibilidade de expansão conforme necessidade operacional.

5.2.4. Interfaces e recursos do hardware:

a) Desempenho em modo *Threat Prevention* (Proteção *Anti-Malware*, IPS e Controle de Aplicação habilitados) mínimo de 9 Gbps;
b) Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 5 Gbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item;
c) Desempenho mínimo de 10 Gbps de IPS;
d) Suporte mínimo de 4.000.000 conexões simultâneas/concorrentes no modo SPI;
e) Suporte mínimo de 115.000 novas conexões por segundo;
f) Deve possuir no mínimo 1 fonte de alimentação. com chaveamento automático de 100-240 VAC;
g) Deve possuir no mínimo 24 interfaces 1 GbE padrão RJ-45;
h) Deve possuir, no mínimo, 6 interfaces 10 GbE SFP+;

i) Deve possuir 1 interface do tipo 1 GbE RJ45 dedicada para gerenciamento do equipamento;
j) Deve possuir ao menos uma interface USB 3.0 (ou superior) com suporte a tecnologias LTE 3G/4G e 5G;
k) A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 500 usuários simultâneos.
l) A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para 500 usuários simultâneos ou mais;
m) Deve suportar, pelo menos, 4000 túneis de VPN tipo *Site-to-Site* padrão IPSEC simultâneos;
n) Deve suportar, no mínimo, 11 Gbps de desempenho de VPN IPSEC;
o) Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante (*datasheet*). A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como o atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame;
p) O fornecimento dos produtos e dos seus licenciamentos devem ser feitos diretamente através da CONTRATADA a qual detém total responsabilidade pelos prazos e garantias estabelecidas neste certame;
q) O Equipamento deverá ser homologado pela ANATEL;
r) Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados;
s) O licenciamento para todos os serviços de *Next Generation Firewall* é totalmente por conta do fornecedor;
t) A garantia do *hardware* é totalmente por conta do fornecedor.

5.2.5. Funcionalidades mínimas obrigatórias do NGFW:

a) Controle de aplicações, com políticas por aplicação, usuário/grupo e categoria;
b) Filtro de URL por categorias e listas personalizadas, com bloqueio por risco;
c) IPS/IDS com assinaturas atualizadas continuamente;
d) Antivírus/*antimalware* de borda e *antispyware* integrados;
e) Controle de acesso por identidade (integração com diretórios/AD/LDAP) e/ou identificação por agentes;
f) Inspeção e controle de tráfego criptografado (SSL/TLS) com políticas por categoria e exceções justificadas;
g) Registro detalhado de tráfego e eventos, com exportação e integração com mecanismos de correlação (SIEM/relatórios do SOC);
h) Atualizações automáticas de *firmware*, patches e assinaturas (com janelas e mecanismos de *rollback*/mitigação);

i) Recursos de segmentação e políticas de segurança por zonas (interna/DMZ/externa), NAT, roteamento e alta disponibilidade lógica quando suportado.

5.2.6. Licenciamento e suporte:

a) Licenciamento para os serviços de NGFW, assinaturas e suporte técnico deverá ser válido por 60 (sessenta) meses, incluindo atualizações de *software*, *firmware* e assinaturas de segurança;
b) Garantia do hardware por 60 (sessenta) meses;
c) A CONTRATADA deverá possuir e apresentar certificação técnica específica dos produtos (hardware, software e serviços) a serem ofertados.

5.2.7. Regras de comprovação técnica:

a) Será exigido *datasheet* oficial do fabricante para comprovação de desempenho e requisitos;
b) Não serão aceitas cartas/declaratórios de fabricante para substituir comprovação objetiva de desempenho por documentação pública do produto;

5.3. Componente 2 - Segurança de *Endpoints* (1.610 *endpoints*, incluindo 10 servidores)

5.3.1. A solução de *endpoint* deverá contemplar proteção para estações de trabalho e servidores incluídos no quantitativo total informado, com gerência centralizada (em nuvem), contemplando proteção contra malware, ransomware e ameaças web, com atualização contínua de assinaturas/motores. A distribuição das licenças se dará por Secretaria, seguindo o seguinte quantitativo:

Quant.	Secretaria
114	SEAD
49	SEDEI
36	SECEL
36	PROCURADORIA
60	SEMA
108	SMDS
60	SEFA
32	GABINETE
490	SESA
486	SED
70	SEPLAN
34	SESP
21	SEOB
14	SESU
1610	**TOTAL (LICENÇAS DE ANTIVÍRUS)**

5.3.2. Funcionalidades mínimas obrigatórias de endpoint:

a) Detecção e bloqueio de vírus, *spyware*, *rootkits* e ameaças correlatas;
b) Proteção contra *ransomware* com mecanismos de contenção/*rollback* quando disponível;
c) Licenciamento básico com chave unitária com número global de usuários;
d) Controle de acesso a dispositivos e mídias removíveis (USB) conforme política;
e) Políticas por grupos/unidades, com herança e exceções;
f) Inventário, visibilidade e relatórios por dispositivo/usuário;
g) Mecanismos de quarentena, isolamento do *host* e ações remotas de resposta;
h) Atualizações automáticas e controle de versões do agente;
i) Segurança para aplicações Google *Workspace;*
j) A integração com Google Workspace deverá ser realizada via API, disponibilizada pelo próprio fabricante da plataforma a ser protegida;
k) Para o Google Workspace, deve ao menos proteger as seguintes aplicações: Gmail e Google Drive;
l) Deve contar com opção de proteção automática para novos usuários criados dentro do espaço empresarial do Google Workspace;
m) A solução deve possuir funcionalidade de auditoria, registrando em log as ações realizadas pelos administradores ou utilizadores da solução;
n) A solução deve entregar, no mínimo, os seguintes recursos de proteção para o Gmail:
    i) Anti-malware, para detecção automática de mensagens contendo conteúdo malicioso.
    ii) Anti-spam, para detecção de e-mails com conteúdo falso ou enganoso, no título da mensagem e corpo do e-mail.
    iii) Anti-phishing, para detecção de links maliciosos no título da mensagem e corpo do e-mail, incluindo ataques de phishing homógrafos.
    iv) Sandbox em nuvem, para análise detalhada de e-mails desconhecidos.
    v) Regras de e-mail, para criação de condições customizadas de filtragem de conteúdo.
o) Para os demais aplicativos de colaboração (OneDrive, SharePoint, Teams ou Google Drive):
    i) Anti-malware, para detecção automática de arquivos contendo conteúdo malicioso.
    ii) Sandbox em nuvem para detecção automática de arquivos desconhecidos.
    iii) Deve possuir painéis para visualização rápida, contendo estatísticas de segurança dos recursos protegidos.
    iv) Além de painéis de visualização rápida pré-definidos, a solução deve permitir a criação de painéis customizados, bem como a edição dos painéis pré-definidos.
p) Geração de relatórios e *dashboards*, com exportação para PDF/CSV, e agendamento de envio por e-mail de relatórios operacionais e executivos.

5.3.3. Gestão da segurança:

a) Funções (RBAC), permitindo delegar diferentes níveis de permissão para a equipe de TI.
b) Instalação Remota e Silenciosa: Capacidade de instalar agentes em estações e servidores de forma remota, sem intervenção do usuário, suportando GPO e SCCM.
c) Remoção Competitiva: Funcionalidade automatizada para desinstalar soluções de antivírus de outros fabricantes já presentes no parque.
d) Operação da Console: a console deve suportar o isolamento de máquinas da rede em caso de infecção, mantendo apenas a comunicação com o servidor de gerenciamento para remediação
e) Console Híbrida Unificada: A solução deve permitir o gerenciamento tanto em nuvem (SaaS) quanto em servidor local (*on-premise*) sem perda de funcionalidades, garantindo alta disponibilidade.
f) Agente Único e Leve: A proteção de estações, servidores e dispositivos móveis deve ser realizada por um único agente de software, otimizado para não consumir mais de 3% de CPU em estado de prontidão e com baixo impacto em memória RAM.
g) Inventário de *Hardware* e *Software*: A console deve realizar automaticamente o inventário de *hardware* e *software* de todos os 1.610 ativos, listando versões de SO, números de série e aplicações instaladas.

5.3.4. Compatibilidade:

a) Sistemas Operacionais Suportados

Categoria	**Sistemas Exigidos (ou posteriores)**
Estações	Windows 10/11, macOS 11+, Ubuntu Desktop 20.04+, Red Hat 8+.
Servidores	*Windows Server* 2022 (*Core* e *Desktop*), Ubuntu/Red Hat Server.
Móveis	Android 6+, iOS 9+, iPadOS 13+.

b) Licenciamento Flexível: A solução não deve impor restrições sobre a quantidade de equipamentos por sistema operacional, permitindo que as licenças sejam distribuídas livremente entre estações, servidores ou dispositivos móveis.
c) Módulos Unificados: Todos os recursos (Antivírus, *Sandbox*, EDR, *proteção de aplicativos Google Woprkspace, defesa contra ameaças móveis, criptografia de discos, segurança de e-mail* e *Patch Management*) devem ser ativados por uma única licença, sem necessidade de *add-ons* separados.
d) Integração com diretórios e autenticação corporativa para aplicação de políticas e correlação de usuários;

e) Possibilidade de suporte a múltiplas plataformas de virtualização, quando pertinente ao ambiente.

5.3.5 Gerenciamento de Vulnerabilidades, Nuvem e Patch Management

a) Varredura Automática de Vulnerabilidades: Identificação contínua de vulnerabilidades (CVEs) em sistemas operacionais e *softwares* de terceiros (Adobe, Java, Browsers, etc.).
b) Correção Automatizada (*Patching*): Capacidade de baixar e instalar as atualizações de segurança diretamente pela console de antivírus, sem necessidade de ferramentas externas, para os 1.610 dispositivos.
c) *Patch Management*: Identificação e correção automatizada de vulnerabilidades no sistema operacional e em aplicações de terceiros (*browsers*, leitores de PDF etc.).
d) *Firewall* e Controle de Dispositivos: *Firewall* bidirecional centralizado e bloqueio/controle granular de pendrives, HDs externos e outros periféricos.
e) Exclusões Inteligentes para Servidores: Reconhecimento automático de funções de servidor (*Active Directory*, *SQL Server*, *Exchange*) para aplicar exclusões de escaneamento que evitem conflitos de performance.
f) Segurança para Google *Workspace* / M365: A solução deve incluir proteção via API para as contas de e-mail corporativo (Gmail) e armazenamento em nuvem (Drive), escaneando anexos e links contra *phishing* e *malwares*.
g) O módulo de gerenciamento de vulnerabilidades e patches deve estar disponível para estações de trabalho e servidores Windows, macOS e Linux
h) Deve rastrear ativamente as vulnerabilidades dos sistemas operacionais suportados e demais aplicações comuns
i) A solução deve oferecer opção para correção manual de determinada vulnerabilidade, bem como, opção para correção automatizada.

5.3.6 Requisitos do Fabricante e Suporte

a) Presença Nacional: O fabricante deve possuir escritório próprio e analistas de pesquisa de ameaças dedicados ao Brasil.
b) Suporte Técnico Nível 3 Nacional: O suporte e atendimento técnico deve ser prestado em português do Brasil, por telefone e e-mail, 24x7 para incidentes críticos. Além disso, os manuais devem ser obrigatoriamente em português do Brasil.
c) Inteligência Local: O fabricante deve possuir laboratórios de pesquisa de ameaças na América Latina e analistas dedicados a ameaças brasileiras.
d) Certificações Internacionais de Segurança:
    i) ISO 27001: Comprovação de que o fabricante segue padrões globais de segurança da informação.
    ii) ISO 9001: Garantia de qualidade nos processos de suporte.
e) Validação por Terceiros: O fabricante deve figurar como "*TopRated*" ou "*Leader*" em testes independentes recentes (como AV-Comparatives, AV-TEST ou MITRE) nos últimos 12 meses.
f) Licenciamento Flexível: Permissão para transferir licenças entre dispositivos conforme a necessidade da administração, respeitando o teto de 1.610 unidades.

5.3.7 Proteção e Detecção Avançada

a) Presença Nacional: O fabricante deve possuir escritório próprio e analistas de pesquisa de ameaças dedicados ao Brasil.
b) Múltiplas Camadas de Defesa: Detecção baseada em *Machine Learning*, Inteligência Artificial, análise heurística e comportamental.
c) *Sandbox* Avançado em Nuvem: Obrigatoriedade de envio automático de arquivos suspeitos (executáveis, scripts, macros de Office) para análise em ambiente isolado (*Sandbox*) do fabricante. A solução deve aguardar o veredito da *sandbox* antes de liberar a execução do arquivo no *endpoint*.
d) Proteção de Baixo Nível (UEFI/BIOS): Capacidade de escanear o *firmware* da máquina (UEFI) antes da inicialização do sistema operacional, para detectar *malwares* persistentes (*rootkits/bootkits*).
e) *Machine Learning* Local e em Nuvem: Uso de algoritmos de aprendizado de máquina que operem mesmo sem conexão à *internet*, complementados por inteligência coletiva em nuvem.
f) Escudo contra *Ransomware*: Módulo específico que monitore comportamentos típicos de criptografia indevida e permita o bloqueio imediato do processo, com capacidade de remediação (*rollback*) de arquivos afetados.
g) EDR (*Endpoint Detection and Response*): Ferramenta integrada para visibilidade total de incidentes, permitindo investigação via gráficos interativos e resposta a ameaças anômalas.
h) Visibilidade Total de Processos: A ferramenta deve registrar cada processo executado, conexões de rede realizadas e alterações no registro do Windows, permitindo a investigação retroativa.
i) Mapeamento MITRE ATT&CK: Todos os incidentes detectados devem ser automaticamente classificados de acordo com a base de conhecimento MITRE ATT&CK, facilitando a compreensão da tática utilizada pelo invasor.
j) Isolamento de *Host*: Capacidade de isolar uma estação ou servidor da rede diretamente pela console, mantendo apenas o canal de comunicação com a gestão para fins de remediação remota.
k) Caça de Ameaças (*Threat Hunting*): Possibilidade de realizar buscas granulares em todo o parque (ex: "quem mais possui este arquivo com este *hash*?") em tempo real.

5.4. Componente 3 - SOC, Operação, *Hardening* e Serviços Especializados (SECaaS)

5.4.1. A contratada deverá fornecer monitoramento ativo 24x7x365, com análise de eventos, detecção e resposta a incidentes e ameaças em tempo real. O serviço deve incluir processos de identificar, proteger, detectar e responder, com evidências rastreáveis e relatórios.

5.4.2. A solução SECaaS deverá incluir, no mínimo:

a) Fornecimento de *hardware* e *software* conforme cenário atual, prevendo crescimento mínimo para o período de vigência;
b) Gestão de licenciamentos e atualizações contínuas de *softwares* e assinaturas;
c) Inclusão e manutenção de regras, políticas de segurança e filtros de conteúdo;

d) *Hardening* contínuo dos ativos de rede e estações para redução de vulnerabilidades;
e) Treinamento especializado para equipe interna quanto à operação e melhores práticas;
f) A execução de 2 (dois) *Pentests* do *firewall* para validação de integridade do perímetro e serviços da prefeitura publicados na WEB durante a vigência do contrato (60 meses), mediante solicitação do Departamento de TI da prefeitura;
g) Relatórios periódicos (operacionais e executivos), com indicadores, incidentes, tendências, ações corretivas e recomendações.
h) A CONTRATADA deverá fornecer infraestrutura de SIEM, no modelo SaaS, contemplando plugins para integração com logs de sistemas Windows, Linux, principais fabricantes de firewall e soluções de endpoint. A solução deverá possuir capacidade de automação (SOAR), inclusive com execução de comandos via API, permitindo, por exemplo, bloqueio automático de endereços IP em firewalls e isolamento de hosts em endpoints, conforme aplicável. Todos os custos de aquisição, subscrição e suporte estarão integralmente a cargo da CONTRATADA.

5.4.3. Requisitos de evidências e rastreabilidade:

a) Registro de chamados, incidentes e ações executadas, com carimbo de tempo e responsável técnico;
b) Relatórios mensais contendo: principais eventos, incidentes, tempo de resposta e resolução, disponibilidade, alterações de regras, *hardening* aplicado, vulnerabilidades mitigadas e pendências;
c) Relatórios sob demanda em situações críticas.

6. REQUISITOS

6.1. Requisitos de sustentabilidade: sempre que aplicável, a solução deverá priorizar mecanismos de eficiência operacional (redução de deslocamentos por suporte remoto quando possível), descarte ambientalmente adequado de materiais substituídos e utilização de embalagens e insumos em conformidade com boas práticas ambientais, sem prejuízo da segurança e disponibilidade do serviço.

6.2. Requisitos de segurança e sigilo:

a) A contratada deverá manter sigilo absoluto sobre quaisquer informações, topologias, credenciais, *logs*, configurações, dados e evidências a que tiver acesso, utilizando-os exclusivamente para execução do contrato;
b) Deverá adotar controles de acesso, segregação de funções e registro de auditoria de sua equipe;
c) É vedada a divulgação de quaisquer informações da contratante;
d) A contratada deverá observar boas práticas compatíveis com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e com padrões reconhecidos de gestão de segurança da informação;
e) Qualquer incidente de segurança envolvendo informações da contratante deverá ser comunicado imediatamente à fiscalização/gestão do contrato, com relatório de impacto e medidas adotadas.

f) Não será permitida a subcontratação dos serviços de monitoramento, detecção e resposta relacionados ao SIEM. A CONTRATADA deverá disponibilizar equipe própria e dedicada para execução dessas atividades, vedando-se o repasse a terceiros, sob qualquer forma.

6.3. Requisitos de continuidade:

a) A solução deve operar *inline*, com mecanismos de contingência operacional compatíveis com a criticidade do serviço;
b) Em situações críticas definidas no SLA, a contratada deverá assegurar capacidade de atendimento físico quando não houver acesso remoto, sem subcontratação/quarteirização.

CAPÍTULO III

DO MODELO DE EXECUÇÃO

7. DESCRIÇÃO DOS SERVIÇOS

7.1. A execução contratual será estruturada em fases, com marcos entregáveis e critérios de aceitação, contemplando as 4 fases abaixo:

Fase 1 - Iniciação e Planejamento (*Kickoff*):

a) Reunião de abertura com definição de responsáveis, governança e canais oficiais;
b) Plano de implantação contendo cronograma, janelas de mudança, matriz de riscos, plano de *rollback* e critérios de aceite;
b) Levantamento técnico (inventário lógico) de *links*, VLANs, regras atuais, serviços publicados, perfis de usuários, *endpoints* e servidores incluídos no escopo.

Fase 2 - Implantação/Configuração (NGFW e *Endpoint*):

a) Instalação física do *appliance* (quando aplicável), integração à rede e configuração de base (zonas, roteamento, NAT);
b) Migração/parametrização de políticas e regras, com validação por amostragem e por cenário;
c) Ativação de assinaturas e serviços (IPS, AV, URL *filtering*, inspeção SSL/TLS conforme política);
d) Implantação do console de *endpoint* (local ou nuvem) e distribuição do agente para 1.610 *endpoints*, incluindo 10 servidores;
e) Definição de políticas de *endpoint*, grupos, exceções e procedimentos de isolamento;
f) Integração com SOC e mecanismos de alertas e correlação de eventos.

Fase 3 - Operação Assistida e Estabilização:

a) Operação assistida por período suficiente para estabilização do ambiente (ajustes finos de regras, falsos positivos, *tuning*);
b) Entrega de documentação "*as built*" (topologia lógica, políticas principais, fluxos críticos, procedimentos de operação e contingência);
c) Treinamento para equipe interna (administração básica e boas práticas);

d) Aceite técnico da implantação mediante *checklist* de conformidade.

Fase 4 - Operação Contínua (SECaaS / SOC 24x7x365):

a) Monitoramento contínuo, detecção e resposta a incidentes;
b) Manutenção e atualização de políticas e assinaturas;
c) *Hardening* contínuo e recomendações;
d) Relatórios mensais e reuniões periódicas de acompanhamento (quando demandado);
e) A execução de 2 (dois) *Pentests* do *firewall* para validação de integridade do perímetro e serviços da prefeitura publicados na WEB durante a vigência do contrato (60 meses), mediante solicitação do Departamento de TI da prefeitura.

7.2. Níveis de serviço (SLA) e tempos máximos:
A contratada deverá atender aos tempos máximos abaixo, contados a partir da abertura do chamado/alerta pelo SOC ou pela contratante, conforme classificação:

GRAVIDADE	Situações (Exemplos)	Tempo de Resposta	Prazo de Resolução Final
Crítico	Parada total de serviços essenciais que impossibilitem o funcionamento de uma ou mais secretarias. Violação de segurança confirmada com impacto em dados ou serviços críticos. Perda de dados ou risco iminente de corrupção em sistemas essenciais. Falha em serviço crítico ou uma das unidades externas sem comunicação/conectividade.	Até 1 hora útil com presença física	Até 2 horas úteis
Alto	Degradação severa de performance em serviços importantes. Falha em serviço crítico ou uma das unidades externas sem comunicação/conectividade.	Até 1 hora útil com presença física	Até 4 horas úteis
Moderado	Falha parcial de um serviço que afeta um número limitado de usuários. Solicitação de ajustes de segurança ou configuração com urgência moderada (Ex: bloqueio de tráfego específico no *firewall*, alteração em ACL de rede).	Até 4 horas úteis	Até 1 dia útil
Baixo	Solicitações de serviço que não impactam a continuidade. Resolução de dúvidas e orientação técnica à equipe de TI da Prefeitura. Geração de relatórios de performance, segurança ou de configuração.	Até 1 dia útil	Até 5 dias úteis
Projetos / Demandas Planejadas	Implementação de novas soluções de infraestrutura. Consultoria para elaboração de projetos de segurança. Execução de atividades complexas que demandam planejamento detalhado.	Até 5 dias úteis (para apresentação de Proposta Técnica (escopo, horas e cronograma)	Conforme Proposta Técnica aprovada pela contratante

7.3. Critérios objetivos de aceitação (principais):

a) *Appliance* instalado/operante e *inline*, com políticas base aplicadas, registro de eventos e atualização ativa;
b) *Endpoints* protegidos com agente instalado e comunicando com console, atingindo 1.610 *endpoints* (incluindo 10 servidores);
c) SOC ativo com geração de alertas, abertura e tratativa de incidentes, relatórios e evidências;
d) Demonstrar possuir equipe especializada para a execução dos *Pentests* mediante atestado de capacidade emitido por, pelo menos, 3 (três) empresas;
e) Documentação entregue (*as built*, procedimentos e relatórios) e treinamento realizado.

8. LOCAL E PRAZO DE ENTREGA/EXECUÇÃO

8.1. Prazo de entrega de até 40 (quarenta) dias úteis, a contar do recebimento da Nota de Empenho e/ou Ordem de Início. Destaca-se aqui que a entrega trata da configuração e ativação dos serviços de segurança de borda (firewall), dos endpoints (antivírus) e da ativação do monitoramento específico destes serviços(SOC).

8.1.1 A CONTRATADA deve apresentar um plano de configuração e ativação dos serviços contratados em um prazo de até 10 (dez) dias úteis a contar do recebimento da Nota de Empenho e/ou Ordem de Início. Este plano deverá ser aprovado pelo Departamento de TI da Prefeitura Municipal de Lajeado.

8.1.2 A entrega e ativação final dos serviços não pode ultrapassar o prazo total discriminado no item 8.1.

8.2. O local de entrega/execução será na Prefeitura Municipal de Lajeado/RS, localizada na rua Júlio May, 242 - 3º andar, em dependências a serem indicadas formalmente pela Administração no início da execução contratual, compatíveis com a infraestrutura de TI e com os pontos de instalação/integração.

8.3. O horário de entrega/execução será: de segunda à quinta-feira, das 08:00 às 11:30 e das 13:30 às 16:45, e na sexta-feira, das 08:00 às 14:00, observado o calendário administrativo municipal e as janelas de mudança previamente aprovadas.

9. OBRIGAÇÕES DA CONTRATANTE

9.1. São obrigações da Contratante:

a) receber o objeto no prazo e condições estabelecidas neste Termo de Referência;
b) verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes neste Termo de Referência e da proposta, para fins de aceitação e recebimento definitivo;
c) comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

d) acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;
e) efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos neste Termo de Referência;
f) a Contratante não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do objeto, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

9.2. Obrigações específicas para este objeto:

a) disponibilizar informações técnicas necessárias (topologia lógica, VLANs, endereçamento, inventário de *endpoints*, regras atuais) e indicar responsáveis para validações;
b) prover acesso controlado às dependências, *racks* e pontos de rede para instalação e manutenção, observadas regras internas;
c) fornecer, quando aplicável, credenciais temporárias e/ou integrações (AD/LDAP) sob gestão da contratante, seguindo boas práticas de mínimo privilégio;
d) aprovar janelas de mudança e acompanhar testes de corte/migração;
e) manter interlocutor técnico e gestor para governança do contrato e aceite de *deliverables*/marcos entregáveis.

10. OBRIGAÇÕES DA CONTRATADA

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

a) efetuar a entrega do objeto em perfeitas condições, novo, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal;
b) responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);
c) comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;
d) manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
e) indicar preposto para representá-la durante a execução do contrato. (enquanto houver contrato);
f) indicar outras obrigações referentes ao objeto no caso concreto.

10.2. Obrigações técnicas e legais específicas (exaustivas):

a) prover, configurar e manter o *appliance* NGFW, licenças, assinaturas e suporte por 60 meses, garantindo atualização contínua de firmware/patches/assinaturas;

b) prover e manter a solução de endpoint para 1.610 endpoints (incluindo 10 servidores), com console de gerenciamento e atualização contínua;
c) executar implantação completa e estabilização, incluindo migração/adequação de políticas, *tuning*, documentação e treinamento;
d) prestar suporte técnico especializado 24x7, com central de atendimento e registros auditáveis (chamados/incidentes);
e) operar SOC 24x7x365, com detecção e resposta proativa, classificando eventos por criticidade e cumprindo SLA;
f) realizar *hardening* contínuo conforme plano aprovado, mantendo registro de alterações e recomendações;
g) Entregar os resultados dos *Pentests*, com relatório técnico analítico que apresente evidências, metodologia, achados (ameaças, vulnerabilidades etc.), criticidade e plano de ação;
h) garantir presença física, sem subcontratação/quarteirização, quando houver impossibilidade de acesso remoto por falha de *link*/*hardware* ou necessidade de troca de mídias físicas, observando o SLA;
i) manter sigilo absoluto sobre informações e configurações da contratante, responsabilizando-se por sua equipe;
j) entregar *datasheets* oficiais do fabricante para comprovação de requisitos e desempenho;
k) manter equipe técnica com qualificação compatível, assegurando continuidade do serviço e atendimento dentro dos prazos;
l) registrar e submeter previamente à aprovação da contratante mudanças relevantes (*change management*), exceto em ações emergenciais de contenção previstas no SLA;
m) Entrega mensal de relatório contendo dados como intercorrências na operação, chamados técnicos abertos e em atendimento, tentativas de ataque, ameaças neutralizadas, conexões perigosas interrompidas etc.

11. DA SUBCONTRATAÇÃO

11.1. É permitida a subcontratação do objeto deste Termo de Referência?
(X) Não.

O objeto da presente contratação não se resume ao mero fornecimento de ativos de rede (hardware), mas engloba uma solução integrada de Security as a Service (SECaaS) de altíssima criticidade, incluindo a gestão de *Next Generation Firewall (NGFW)*, proteção de *endpoints/servidores* e, primordialmente, o monitoramento contínuo por meio de um Security Operation Center (SOC) 24x7x365 e a execução de testes de intrusão (*Pentests*).

Trata-se de serviços de natureza predominantemente intelectual e estratégica, que exigem alto grau de especialização, fidúcia (confiança) e integração contínua. A dispersão dessas responsabilidades por meio de subcontratação fragmentará a execução do ecossistema de segurança, comprometendo a eficácia das barreiras de defesa do órgão.

12. GARANTIA (E/OU VALIDADE)

(X) O prazo de garantia do objeto contra falhas, erros e defeitos, pelo seu caráter de prestação de serviço contínuo, durante toda a vigência do contrato, a contar da entrega ou ativação definitiva, independentemente da garantia oficial do fabricante de produtos ou equipamentos utilizados pela CONTRATADA.

(X) O prazo de garantia para os serviços de instalação, deverá ser igual a vigência do contrato, a contar do recebimento definitivo.

(X) Durante todo o período do contrato, a ADJUDICATÁRIA obriga-se a efetuar, sem ônus para a Prefeitura Municipal de Lajeado/RS, a substituição ou reparo do objeto que apresentar defeitos de operação, no prazo de até 4 horas, a contar da primeira hora do atendimento inicial.

CAPÍTULO IV

DO MODELO DE GESTÃO DO CONTRATO

13. CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

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

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

13.3. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

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

13.5. Os responsáveis pela fiscalização do contrato serão os seguintes servidores:

- Fiscais técnicos: Cristiano André Lenz, matrícula 6978, contactável através do e-mail cristiano.lenz@lajeado.rs.gov.br e Marcelo de Aguiar Mendes, matrícula 14197, contactável através do e-mail marcelo.mendes@lajeado.rs.gov.br e telefone (51) 3982-1012;
- Fiscal administrativo: Cristiano Rafael Pinto, matrícula 17256, contactável através do e-mail cristiano.pinto@lajeado.rs.gov.br , telefone (51) 3982-1012;

13.6. O gestor responsável pelo contrato:

- Secretária da Administração, Patrícia Haenssgen, patricia.haenssgen@lajeado.rs.gov.br, ramal 1006.

14. TESTES, INSPEÇÕES E VERIFICAÇÕES

14.1. A Contratante poderá realizar testes e inspeções para verificar se os bens e/ou serviços fornecidos atendem às especificações estabelecidas neste Termo de Referência.

14.2. No caso de não conformidade, a Contratada será notificada para que tome as medidas corretivas necessárias, sem prejuízo da aplicação das sanções previstas neste Termo de Referência.

CAPÍTULO V

DO MODELO DE MEDIÇÃO E PAGAMENTO

15. CONDIÇÕES DE RECEBIMENTO

15.1. O recebimento do objeto deverá observar o disposto no art. 140, da Lei nº 14.133/2021, e será realizado por servidor ou comissão designada pela autoridade competente, mediante termo circunstanciado.

15.2. O objeto será recebido:
a) provisoriamente, para efeito de posterior verificação da conformidade com as especificações constantes neste Termo de Referência e da proposta;
b) definitivamente, após a verificação da qualidade e quantidade do material e consequente aceitação.

15.3. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato.

15.4. O recebimento definitivo ocorrerá após a verificação do atendimento às especificações, condições e critérios estabelecidos neste Termo de Referência, inclusive quanto aos entregáveis técnicos, evidências, relatórios, treinamento e aceite operacional.

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

15.6. Só serão aceitos equipamentos novos, sem avarias, arranhões, sinais de uso prévio, recondicionamento ou adaptações não homologadas pelo fabricante;

15.7 Deverão estar de acordo com as especificações descritas no item 5.2 deste termo de referência;

15.8 Os quantitativos deverão estar de acordo com o solicitado pela CONTRATANTE, respeitando os limites máximos do contrato;

15.9 O recebimento definitivo ocorrerá de forma tácita e de acordo com os prazos constantes no item 8.1, confirmado após a aferição da qualidade dos equipamentos e serviços executados mediante aceite formal realizado pelo Departamento de TI.

16. DAS SANÇÕES ADMINISTRATIVAS

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

a) dar causa à inexecução parcial do contrato;

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

c) dar causa à inexecução total do contrato;

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

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

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

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

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

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

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

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

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

17. DAS PENALIDADES

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

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

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

b) multa monetária;

c) rescisão de contrato;

d) suspensão do direito de licitar junto ao Município de Lajeado/RS;

e) declaração de inidoneidade para contratar ou transacionar com o Município de Lajeado/RS.

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

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

17.4. A critério da autoridade competente, a aplicação de quaisquer penalidades acima mencionadas acarretará perda da garantia e todos os seus acréscimos.

17.5. Para os atrasos de entrega relativos à implantação do projeto, o não cumprimento dos prazos acordados implicará na aplicação de multa diária considerada

sobre o faturamento médio mensal, obtido a partir dos valores da proposta vencedora, calculados da seguinte forma:

- 1% para cada dia em que os serviços da estrutura lógica do projeto não estiverem entregues e concluídos;
- 1% para cada dia em que o sistema de chamados não estiver ativo e disponível para uso;
- além das multas acima previstas, outras sanções também podem culminar no cancelamento do contrato, sem prejuízo às demais sanções aplicáveis.

17.6. Será aplicada multa de 0,3% (três décimos por cento) do valor total corrigido do contrato, por dia de não fornecimento dos serviços.

17.7. Será aplicada multa de 10% (dez por cento) sobre o valor corrigido do contrato, quando a licitante vencedora:

a) prestar informações inexatas ou causar embaraços à fiscalização;
b) transferir ou ceder obrigações, no todo ou em parte a terceiros, sem prévia autorização da contratante;
c) executar o objeto deste certame em desacordo com as especificações ou normas técnicas, independentemente da obrigação de fazer as correções necessárias às suas expensas;
d) desatender às determinações da fiscalização;
e) cometer qualquer infração às normas legais federais, estaduais e municipais por meios culposos e/ou dolosos, fraude fiscal no recolhimento de qualquer tributo, encargos sociais, ou previdenciários, respondendo ainda pelas multas aplicadas pelos órgãos competentes em razão da infração cometida, cabendo a Prefeitura o direito de exigir a Folha de Pagamento dos empregados a qualquer momento;
f) não iniciar, sem justa causa, execução dos serviços ou não fornecer os materiais contratados no prazo fixado, estando sua proposta dentro do prazo de validade;
g) ocasionar sem justa causa, atraso superior a 03 (três) dias na execução dos serviços contratados ou fornecimento de materiais;
h) recusar-se a executar, sem justa causa, no todo ou em parte os serviços ou fornecimento contratados;
i) praticar por ação ou omissão, qualquer ato que por imprudência, negligência, imperícia, dolosamente ou não, venha a causar danos à contratante ou a terceiros, independente da obrigação da contratada em reparar os danos causados.

17.8. A causa determinante da multa deverá ficar plenamente comprovada e o fato a punir comunicado por escrito pela fiscalização à direção do órgão.

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

17.10. Será aplicada a sanção de declaração de inidoneidade para licitar ou contratar com a Administração Pública, ao responsável pelas infrações administrativas previstas nos incisos VIII, IX,X, XI e XII do caput do art. 155 da Lei n.º 14.133/2021, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do caput do referido artigo que justifiquem a imposição de penalidade mais grave que a sanção referida no § 4º do art. 155 da mesma Lei, e impedirá o responsável de licitar ou contratar no âmbito da

Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos;

17.11. As sanções previstas nos incisos I, III e IV, do § 1º, art. 155 da Lei n.º 14.133/2021 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

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

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

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

17.14.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

17.15. Em situações de não cumprimento do nível de acordo de serviço, serão aplicadas as seguintes multas para cada ocorrência não atendida, ou atendida fora do prazo:

GRAVIDADE	MULTA
Incidentes Críticos	R$ 5.000,00
Incidentes Altos	R$ 3.000,00
Incidentes Moderados	R$ 1.000,00
Incidentes Baixos	R$ 200,00

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

18. FORMA DE PAGAMENTO

18.1. O pagamento será efetuado em favor da Contratada, mediante apresentação de nota fiscal e demais documentos exigidos, após o recebimento definitivo do objeto e atesto do fiscal do contrato, observadas as condições previstas neste Termo de Referência.

18.2. O pagamento será realizado por meio de ordem bancária, na conta indicada pela Contratada, vedada a cobrança de taxas adicionais não previstas.

18.3. O pagamento será efetuado no prazo de até 10 (dez) dias úteis após a liquidação da despesa, detalhando o objeto fornecido, com o devido recebimento e a aprovação do fiscal do contrato, de acordo com o empenho, por meio de depósito bancário.

18.4. Somente será efetuado o pagamento mediante apresentação da Negativa do FGTS e INSS.

18.5. No ato do pagamento, serão efetuadas as retenções tributárias e previdenciárias previstas na legislação pertinente.

18.6. A nota fiscal/fatura emitida pelo fornecedor deverá conter, em local de fácil visualização, a indicação do número do empenho, a fim de acelerar a liberação do documento fiscal para pagamento.

18.7. Poderá o Município de Lajeado/RS compensar multas aplicadas com valores contratados e ainda não pagos.

18.8. Somente será autorizado o pagamento, pela autoridade competente, à fornecedores que estiverem quites com a Fazenda Municipal de Lajeado/RS. (Art. 2º, V, do Decreto Municipal nº 12.513/2022).

18.9. O pagamento de cada item só se iniciará após a implantação total da solução.

19. OBRIGAÇÕES TRIBUTÁRIAS

19.1. A Contratada é responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato.

20. CONDIÇÕES DE PAGAMENTO

20.1. O prazo de pagamento será de 10 (dez) dias úteis, contados da data do atesto do recebimento definitivo e da apresentação da nota fiscal/fatura, desde que atendidas as condições previstas neste Termo de Referência.

20.2. Em caso de irregularidades na documentação, o prazo de pagamento será contado a partir da sua regularização.

20.3. Poderão ser realizadas retenções tributárias na forma da legislação aplicável.

21. DO REAJUSTE

21.1. Os preços contratados poderão ser reajustados, observado o intervalo mínimo de 12 (doze) meses, contados a partir da data do orçamento estimado, nos termos da legislação aplicável.

21.1.1. O reajuste será calculado pelo índice definido anualmente pela Administração Municipal.

21.2. O reajuste, quando cabível, dependerá de formalização processual e justificativa, com comprovação e análise de vantajosidade.

22. DO REEQUILÍBRIO ECONÔMICO-FINANCEIRO

22.1. Poderá ser concedido reequilíbrio econômico-financeiro nos casos previstos em lei, mediante requerimento formal e comprovação, nos termos da Lei nº 14.133/2021.

CAPÍTULO VI

DA SELEÇÃO DO FORNECEDOR

23. MODALIDADE, TIPO DE LICITAÇÃO E CRITÉRIO DE JULGAMENTO

23.1. Considerando as características do objeto, a contratação será de forma licitação, na modalidade Pregão Eletrônico, com fundamento no art. 28, inciso I, da Lei nº 14.133/2021.

23.2. O critério de julgamento será o de menor preço, com verificação de conformidade técnica aos requisitos deste Termo de Referência.

23.3. A adjudicação deverá assegurar a contratação de solução integrada, com atendimento integral ao escopo e ao SLA.

24. CONDIÇÕES DE PARTICIPAÇÃO

24.1. Poderão participar do certame empresas legalmente constituídas e que atendam às condições de habilitação e qualificação definidas neste Termo de Referência e no edital.

25. DOCUMENTAÇÃO E HABILITAÇÃO

25.1. Será exigido atestado de capacidade técnica?
(X) Sim. Justifique e descreva:

Será exigida comprovação de aptidão técnica por meio de atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, demonstrando que a licitante já executou serviços compatíveis com o objeto, contemplando, no mínimo: fornecimento/gestão de *firewall* NGFW e/ou SECaaS, proteção de *endpoints* e/ou operação de SOC, com comprovação de atendimento a SLA e suporte 24x7, em quantidades e complexidade equivalentes, admitida a soma de atestados, desde que compatíveis e coerentes com o escopo.

25.2. Será exigida visita técnica?
( ) Não.
( ) Sim.
( ) Opcional.
(X) Obrigatória. Justifique a necessidade de vistoria obrigatória:

A visita técnica será obrigatória; não será facultativa, pois é imprescindível que as licitantes conheçam o ambiente e planejem adequadamente implantação, integrações e eventuais janelas de mudança. A não realização de visita técnica não poderá ser utilizada como justificativa para descumprimento de prazos, falhas de dimensionamento ou pedidos posteriores de aditivos por desconhecimento do ambiente. Deve obrigatoriamente ser realizada por profissional técnico especialista e com vínculo empregatício comprovado com o FORNECEDOR.

25.3. Será exigido *datasheet*/catálogo do fabricante?
(X) Sim. Descreva:

Será exigida a apresentação de *datasheet*/catálogo oficial do fabricante, público e verificável, contendo especificações técnicas, desempenho, interfaces e características do *appliance* NGFW e dos componentes de *endpoint*/console, bem como informações de

licenciamento e serviços. O *datasheet* será utilizado para conferência objetiva de conformidade. Não serão aceitas cartas/declarações para comprovar desempenho quando houver documentação oficial aplicável.

25.4. Legislação técnica, normas e boas práticas aplicáveis (quando pertinentes ao objeto):
a) Lei nº 13.709/2018 (LGPD), no que tange a tratamento e proteção de dados pessoais;
b) ABNT NBR ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação) e ABNT NBR ISO/IEC 27002 (controles);
c) ABNT NBR ISO/IEC 27005 (gestão de riscos) e ABNT NBR ISO/IEC 27035 (gestão de incidentes);
d) NIST SP 800-61 (*Computer Security Incident Handling Guide*);
e) NIST SP 800-115 (*Technical Guide to Information Security Testing and Assessment*) para diretrizes de testes e avaliações;
f) OWASP *Testing Guide* (para metodologia de testes aplicável a vetores *web* quando incidentes envolverem aplicações);
g) CIS *Controls* (controles de segurança recomendados), como referência de *hardening* e maturidade;
h) Normas e RFCs correlatas a IPsec/SSL/TLS quando aplicáveis às configurações de VPN (sem prejuízo de outras referências técnicas aceitas);

i) ISO/IEC 27001 que define *como* montar o Sistema de Gestão de Segurança da Informação (SGSI). É a única norma passível de certificação.

j) ISO/IEC 27002 (antiga 17799) boas práticas (o "código de prática") e os controles de segurança que você seleciona para atender aos requisitos da 27001.

25.5. Será exigida amostra?
(X) Não.
( ) Sim. Justifique e descreva:

25.6. Habilitação Jurídica, Regularidade Fiscal e Trabalhista e demais documentos: deverão ser apresentados conforme exigências do edital, legislação aplicável e itens padronizados do Município, incluindo as declarações e certidões pertinentes.

25.7. A apresentação de documentos falsificados ou adulterados acarretará a emissão de declaração de inidoneidade e sujeitará a empresa às penalidades previstas no item 17.

25.8. Quando da apresentação definitiva deverão os documentos ser apresentados em uma única via, datilografados ou digitados, não apresentando emendas, rasuras, entrelinhas ou forem ilegíveis

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

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

25.10. Os documentos que dependam de prazo de validade e que não contenham esse prazo especificado no próprio corpo, em lei ou neste processo, devem ter sido expedidos em no máximo 90 (noventa) dias anteriores à data determinada para a entrega dos envelopes.

25.11. Os documentos deverão ser apresentados em cópias acompanhadas do original, por qualquer processo de cópia autenticada por cartório competente ou por servidor desta municipalidade. Ressalta-se que cópias apresentadas em papel térmico de FAX não serão aceitas, nem tampouco autenticação de cópias pela via autenticada.

25.11.1. Os documentos emitidos via internet terão sua autenticidade confirmada através de consulta ao site do órgão emissor.

26. PROVA DE CONCEITO (PoC) / TESTE DE CONFORMIDADE

Para este objeto, além da POC, a conformidade técnica será verificada por análise documental (*datasheets* oficiais), validação de requisitos e, quando pertinente, por testes e inspeções durante a implantação/recebimento, conforme itens 14 e 15 deste Termo de Referência.

A **Prova de Conceito (POC)** tem por objetivo validar a eficácia, o desempenho e a conformidade da solução de **Security as a Service (SECaaS)** ofertada. O procedimento visa garantir que a ferramenta suporte a volumetria e a complexidade inerentes às demandas de segurança da informação da Prefeitura Municipal de Lajeado.

26.1. Cronograma e Carga Horária

A execução da POC deverá observar o prazo máximo de **02 (dois) dias úteis**, totalizando **04 (quatro) turnos** de trabalho. As atividades ocorrerão obrigatoriamente dentro do horário de expediente do Departamento de TI do Município, conforme a seguinte distribuição:

- **Preparação e Configuração:** até 03 (três) turnos destinados ao setup do ambiente, parametrizações e ajustes técnicos necessários.
- **Avaliação e Demonstração:** 01 (um) turno final dedicado à apresentação formal dos resultados e avaliação técnica pela comissão competente.

26.2. Dos Pilares de Avaliação

Para fins de aceite, a solução será submetida a testes estruturados em quatro eixos fundamentais:

1. **Desempenho de Rede:** Capacidade de tráfego, latência e disponibilidade.
2. **Eficácia de Proteção:** Resiliência contra ameaças e precisão dos mecanismos de defesa.
3. **Gestão de Ativos e Vulnerabilidades:** Visibilidade do parque tecnológico e acurácia na identificação de falhas.
4. **Operação de SOC (Security Operations Center):** Capacidade de monitoramento, resposta a incidentes e inteligência operacional.

26.3. Das Excepcionalidades Técnicas

Caso a licitante vencedora seja impossibilitada de demonstrar a comprovação funcional de qualquer requisito devido a limitações ou instabilidades na infraestrutura de TI da **CONTRATANTE**, aplicar-se-á o seguinte rito:

- A impossibilidade deverá ser analisada e atestada pela equipe técnica do Departamento de TI da Prefeitura.
- Uma vez autorizada, a comprovação do requisito poderá ser suprida mediante a apresentação de **documentação técnica oficial do Fabricante** da solução.

26.4. Das Normas de Conduta e Contestações

Durante a realização da POC, é estritamente vedado a outras empresas concorrentes interpelar, questionar ou interferir nas atividades dos técnicos da empresa vencedora, nem tampouco nas atividades da equipe técnica da prefeitura.

Quadro dos elementos a serem avaliados na POC

Categoria	Item de Teste / Funcionalidade	Procedimento de Avaliação	Resultado Esperado (Critério de Sucesso)
1. Hardware e Performance	**Capacidade das Interfaces e Rack**	Verificar fisicamente se o appliance é 1U e possui 24 portas 1GbE e 6 portas 10GbE SFP+.	Conformidade total com o item 5.2.4 do TR.
1. Hardware e Performance	**Stress Test: Throughput Real**	Injetar tráfego simulado com **Inspeção SSL e Threat Prevention** ativos.	Manter estabilidade próxima aos **5 Gbps (SSL)** e **9 Gbps (TP)** exigidos.
1. Hardware e Performance	**Alta Disponibilidade (HA)**	Simular falha de energia ou desconexão de cabo no appliance (se em cluster).	Comutação de tráfego sem queda de sessões ativas (zero downtime).
2. Segurança NGFW	**SD-WAN e Balanceamento**	Configurar dois links de internet e simular a queda de um deles durante uma chamada de voz/vídeo.	Transição transparente sem queda da aplicação (Jitter/Latência controlados).

2. Segurança NGFW	**Filtragem de Tráfego Criptografado**	Tentar aceder a um site malicioso via HTTPS com o certificado de inspeção instalado.	O Firewall deve decifrar, identificar a ameaça e bloquear o acesso.
3. Endpoint (EPP/EDR)	**Anti-Ransomware com Rollback**	Executar um simulador de criptografia numa máquina de teste isolada.	Bloqueio imediato do processo e reversão automática dos ficheiros afetados.
3. Endpoint (EPP/EDR)	**Controlo de Dispositivos (USB/BT)**	Tentar copiar ficheiros para um dispositivo USB não autorizado.	Bloqueio da cópia e geração de log na consola centralizada.
3. Endpoint (EPP/EDR)	**Integração Google Workspace**	Configurar a proteção para o domínio da Prefeitura no Google Drive/Gmail.	Detecção de malware em ficheiros armazenados na nuvem e anexos de e-mail.
4. Gestão e Vulnerabilidades	**Patch Management Automático**	Identificar softwares desatualizados (ex: Chrome, Java) e disparar atualização via console.	Instalação silenciosa do patch sem intervenção do utilizador final.
4. Gestão e Vulnerabilidades	**Inventário de Ativos (Hardware/SW)**	Gerar relatório automático de hardware (CPU, RAM, Disco) de 5 máquinas de teste.	Relatório preciso e em tempo real, conforme item 5.3.6 do TR.
5. Operação e SOC	**Simulação de Incidente (SOC 24x7)**	Simular um ataque de força bruta ou movimento lateral às 22h ou fim de semana.	Notificação do SOC num tempo inferior ao SLA estabelecido (ex: 15-30 min).
5. Operação e SOC	**Visibilidade SIEM SaaS**	Aceder ao portal de logs e correlacionar um evento de rede (FW) com um evento de host (EP).	Visualização da "Timeline" completa do ataque num único dashboard.

Quaisquer manifestações, dúvidas ou contestações de terceiros deverão ser formalizadas exclusivamente por meio dos canais oficiais previstos no processo licitatório, respeitando os prazos legais de recursos.

CAPÍTULO VII

DISPOSIÇÕES GERAIS

27. ESTIMATIVA DE PREÇOS

27.1. A estimativa de preços deverá ser elaborada com base em parâmetros legalmente admitidos, conforme art. 23, § 1º, inciso IV da Lei nº 14.133/2021, que, para este edital foi feita por meio de pesquisa direta com 3 (três) fornecedores, mediante solicitação formal de cotação a empresas idôneas e com reconhecida atuação na área de Segurança da Informação. Ressalta-se aqui que foi realizada consulta no site oficial do PNCP e não foi localizado objeto equivalente ao discriminado no presente Termo de Referência.

27.2. A estimativa de preços é apresentada abaixo e as propostas dos valores obtidos serão juntadas ao processo administrativo como anexos específicos de "Pesquisa de Preços", contendo os preços unitários referenciais, vinculando-se aos itens do objeto deste TR.

Tabela de itens para vinculação da estimativa (valores e fontes constarão no anexo de pesquisa de preços):

Item	Descrição	Unidade	Quantidade	Fonte do preço referencial	Observação
1	*Appliance* NGFW (01 un) com licenças/assinaturas e suporte	un	1	3 fornecedores especializados	Não encontrado equivalente no PNCP
2	Licenças de *endpoint* (estações)	lic	1600	3 fornecedores especializados	Não encontrado equivalente no PNCP
3	Licenças de *endpoint* (servidores)	lic	10	3 fornecedores especializados	Não encontrado equivalente no PNCP
4	Serviços SECaaS (SOC 24x7x365, suporte, *hardening*, treinamento)	sv	1	3 fornecedores especializados	Não encontrado equivalente no PNCP
5	*Pentests* do *firewall e serviços publicados na WEB*	sv	2	3 fornecedores especializados	Não encontrado equivalente no PNCP

Tabela de itens para vinculação da estimativa (valores e fontes constarão no anexo de pesquisa de preços):

Orçamento: Audere Comercio em tecnologia da Informação LTDA					
Descrição	**Qtde**	**UN**	Valor Mensal	Valor Anual	Total 60 meses

Solução integrada de segurança cibernética em modalidade SECaaS (Segurança como serviço - Security as a Service)	60	mês	R$ 39.990,00	R$ 479.880,00	R$ 2.399.400,00

Orçamento: CTINET SOLUÇÕES EM CONECTIVIDADE E INFORMÁTICA LTDA					
Descrição	**Qtde**	**UN**	Valor Mensal	Valor Anual	Total 60 meses
Solução integrada de segurança cibernética em modalidade SECaaS (Segurança como serviço - Security as a Service)	60	mês	R$ 39.073,00	R$ 468.876,000	R$ 2.344.380,00

Orçamento: SCL SECURITY SERVICOS DE INFORMATICA LTDA					
Descrição	**Qtde**	**UN**	Valor Mensal	Valor Anual	Total 60 meses
Solução integrada de segurança cibernética em modalidade SECaaS (Segurança como serviço - Security as a Service)	60	mês	R$ 35.420,00	R$ 425.040,00	R$ 2.125.200,00

Também foi feita uma busca de preços no PNCP, contudo não foi possível localizar propostas que atendam às demandas e ao objeto deste pleito.

Para a definição do valor, foi realizada a média simples dos três orçamentos, com arredondamento para reduzir o número de casas decimais dos valores unitários por licença.

Descrição	**Uidade**	Valor mensal	Total anual	Total em 60 meses
Solução integrada de segurança cibernética em modalidade SECaaS (Segurança como serviço - *Security as a Service*)	mês	R$ 38.157,00	R$ 457.932,00	R$ 2.289.660,00

28. DOTAÇÃO ORÇAMENTÁRIA

28.1. As despesas decorrentes desta contratação correrão por conta de dotação orçamentária própria, a ser consignada no orçamento vigente, observada a disponibilidade orçamentária e financeira.

28.2. Dotação orçamentária: será indicada *a posteriori* pela unidade competente no processo de formalização, quando da emissão da Nota de Empenho, com a respectiva reserva orçamentária.

29. DISPOSIÇÕES FINAIS

29.1. O presente Termo de Referência integra o processo de contratação e deverá ser observado pela Contratada durante toda a execução, prevalecendo suas condições técnicas e operacionais.

29.2. As dúvidas e omissões serão dirimidas pela Administração, observada a legislação aplicável e os princípios da Administração Pública.

29.3. O foro competente para dirimir eventuais controvérsias será o da Comarca de Lajeado/RS, com renúncia a qualquer outro, por mais privilegiado que seja.

Lajeado/RS, 19 de janeiro de 2026.

Responsável pela Elaboração: Luis Antônio Schneiders

Função: Diretor de Governo - Coordenadoria de TI e modernização Administrativa

Autoridade Competente: Patrícia Haenssgen

Cargo: Secretária de Administração

ANEXO I - Modelo de Proposta Comercial

PROPOSTA COMERCIAL
PREGÃO ELETRÔNICO Nº XX/2025
NOME DA PROPONENTE:
CNPJ:
ENDEREÇO:
TELEFONE/FAX:
E-MAIL:

OBJETO: O presente Termo de Referência tem por objeto disciplinar a contratação de solução integrada de segurança cibernética em modalidade SECaaS (*Security as a Service*), contemplando: fornecimento em regime de locação/aluguel de 01 (um) appliance de *Firewall* do tipo *Next Generation Firewall* (NGFW), licenciamento e proteção de até 1610 (mil seiscentos e dez) endpoints (incluindo até 10 (dez) servidores como endpoints), serviços de implantação, configuração, migração/adequação, operação assistida, suporte técnico especializado, monitoramento SOC 24x7x365, *hardening* contínuo, treinamento para equipe interna e realização de 2 *Pentests* durante a vigência do contrato. Lote único.

Especificação dos itens que compõem o objeto da contratação

Descrição	**Uidade**	Valor mensal	Total anual	Total em 60 meses
Solução integrada de segurança cibernética em modalidade SECaaS (Segurança como serviço - *Security as a Service*)	mês			

Para a construção da proposta para o Objeto apresentado no quadro acima, devem ser observados no mínimo a entrega dos itens apresentados no abaixo.

Detalhamento do Objeto para composição do valor do serviço

Item	**Descrição**	**Un**	**Quantidade**
1	*Appliance* NGFW (*rack-mount*) com licenças/assinaturas e suporte	un	1
2	Licenciamento e proteção de *endpoints* (estações de trabalho e *notebooks*) - Antivírus	lic	1.600
3	Licenciamento e proteção de *endpoints* (servidores) incluídos no quantitativo total	lic	10
4	Serviços SECaaS: implantação, operação assistida, suporte, SOC 24x7x365, *hardening* e treinamento	sv	1
5	*Pentest* do *firewall* e serviços publicados na WEB	sv	2

VALOR GLOBAL PARA O LOTE ÚNICO: R$ _____ (valor por extenso)
PRAZO DE VALIDADE DA PROPOSTA: 60 (sessenta) dias, contados da data de sua apresentação.

A licitante, por intermédio de seu representante legal abaixo identificado, para todos os efeitos legais e administrativos, sob as penas da lei, DECLARA:

1. Que se responsabiliza pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, não cabendo à Prefeitura responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

2. Que seu(s) sócio(s), dirigente(s) ou administrador(es) não é(são) servidor(s) ou dirigente(s) da Prefeitura e não possui(em) vínculo familiar (cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau, nos termos dos artigos 1.591 a 1.595 da Lei nº 10.406/2002 – Código Civil) com:

- Servidores(s) detentor(es) de cargo comissionado que atue(m) em área da Prefeitura com gerenciamento sobre o contrato ou sobre o serviço objeto da presente licitação;
- Servidores(s) detentor(es) de cargo comissionado que atue(m) na área demandante da licitação;
- Servidores(s) detentor(es) de cargo comissionado que atue(m) na área que realiza a licitação;
- Autoridade da Prefeitura hierarquicamente superior às áreas supramencionadas.

3. Que não tem e que não contratará prestador(es) para a execução de serviço objeto desta licitação com vínculo familiar (cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau) com servidores(s) da Prefeitura que exerçam cargo em comissão ou função de confiança ou com servidores(s) efetivos da Prefeitura:

- Em área da Prefeitura com gerenciamento sobre o contrato ou sobre o serviço objeto da presente licitação e/ou contrato;
- Na área demandante da licitação;
- Na área que realiza a licitação.

Local e Data. __ / _____ / ____

_____
NOME DO REPRESENTANTE LEGAL
CPF xxxxxxxxx / RG xxxxxxxxx
CARGO/VÍNCULO

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: IDEE.SSYK.USAC.JAOL

Este documento foi assinado eletronicamente pelos seguintes signatários nas datas indicadas (horário de Brasília)

- Assinado eletronicamente por LUIS ANTONIO SCHNEIDERS, Diretor(a) de Governo, em 10/07/2026 13:51:58 pela Portaria 33.676 de 14/02/2025

- Assinado eletronicamente por PATRICIA HAENSSGEN, Secretário(a) de Administração, em 10/07/2026 13:55:45 pela Portaria 33473

Verifique a autenticidade em www.lajeado.rs.gov.br/autenticacao com a chancela IDEE.SSYK.USAC.JAOL