Estudo Técnico Preliminar (ETP)

1. Descrição da Necessidade

O presente ETP visa estabelecer as diretrizes e requisitos para a contratação de serviços especializados de segurança de borda na forma de Firewall, segurança de endpoints (antivírus) e monitoramento (SOC) em modalidade SECaaS (Security as a Service), incluindo hardware em modalidade de aluguel, licenciamentos, atualizações, suporte 24x7, treinamento, hardening e Pentest semestral.

O contrato atual está legalmente esgotado, fato que exige a abertura de nova competição pública (licitação) que, por outro lado, também permite explorar novas soluções de mercado com potencial de atender as demandas atuais e futuras da Prefeitura.

A aquisição de uma nova solução de segurança é essencial para assegurar a conformidade com regulamentações de segurança, proteger dados sensíveis e mitigar os riscos associados a ataques cibernéticos, assegurando assim, pelo menos, os princípios de Confidencialidade, Integridade e Disponibilidade das operações administrativas e dos serviços públicos.

2. Análise das Contratações Anteriores

Para fins de caracterização das contratações anteriores, são apresentados dois contratos, os quais refletem os 6 anos anteriores.

a) A solução anterior de firewall foi estabelecida com base no Contrato nº 037-04/2020, firmado em 17 de março de 2020, que especifica a aquisição de uma plataforma integrada de segurança da informação do tipo appliance com hardware adquirido e tombado pela Prefeitura. Os softwares, além da contratação inicial, já foram renovados em duas oportunidades e dentro dos preceitos legais da Lei 8.666. Esta solução, embora robusta para o período inicial de uso, apresenta limitações crescentes devido à obsolescência tecnológica e ao aumento das demandas modernas de segurança. com o fim da vigência do contrato legal de 60 meses, a necessidade de um novo processo de licitação tornou-se obrigatório, contudo, também contribui para assegurar a continuidade operacional e a proteção contra as ameaças mais recentes e também analisar o mercado para compreender a possibilidade de novas formas de contratação. A contratação foi realizada através do Contrato nº 037-04/2020, no valor total inicial de R$280.000,00, cobrindo aquisição, licenças, suporte técnico, atualizações e treinamento pelo período de 36 meses. Houve uma segunda renovação de 12 meses no ano de 2023 e uma última contratação feita no ano de 2024 com o valor de R$105.675,00 pelo período de 12 meses, porém somente para licenças de software e serviços, visto que o hardware é de propriedade do Município. O valor atual desta solução varia em torno de R$ 120.000,00 por ano.

b) Solução de segurança para endpoints (antivírus) estabelecida com base no contrato Nº 72-01/2025, o qual prevê a instalação de licenças e vacinas antivírus em todos os computadores pessoais (notebooks e PCs) corporativos com valor aproximado de R$ 90.000,00 por ano. Legalmente já não é possível estender novos períodos para este contrato.
c) A solução atual, contratada em maio/2025, estabelece a contratação de serviços especializados na forma de Firewall em modalidade SECaaS (Security as a Service) com valor de R$ 60.000,00 por ano. Este contrato abrange o fornecimento de equipamentos (hardware) em comodato e respectivos softwares de segurança, licenciamentos e atualizações (patches, firmware, assinaturas de segurança) por período mínimo de 12 (doze) meses, serviços de implantação, criação, configuração, e manutenção das políticas e regras de segurança, migração de dados (quando necessário), monitoramento e aplicação de contramedidas em regime de 24x7 (vinte e quatro horas, sete dias por semana), suporte técnico especializado, incluindo manutenção preditiva, corretiva e evolutiva, com SLA conforme descrito neste Termo de Referência, criação e manutenção de regras de segurança, treinamento para equipe interna da Prefeitura Municipal de Lajeado, assegurando autonomia básica na administração do ambiente de segurança e hardening contínuo e Pentest de firewall semestral, de modo a garantir a eficácia das políticas e regras de segurança, bem como a mitigação de riscos.

Pontos Positivos:

- Atendimento às demandas iniciais de segurança.
- Solução reconhecida no mercado por sua competência.
- Representante oficial do fabricante sediado em Porto Alegre.
- Presença de funcionalidades de firewall de próxima geração.
- Suporte técnico.

Pontos Negativos:

- Impossibilidade legal de estender os contratos vigentes.
- Obsolescência já estipulada para o ano de 2028 quando deixará de receber novas atualizações de software e serviços.
- Limitações na escalabilidade para atender às demandas emergentes de aplicações em vistas do hardware entrar em fase de defasagem tecnológica.
- Possibilidade de ocorrência de falhas em virtude do longo tempo de uso.
- A versão adquirida pela Prefeitura não suporta alta disponibilidade, o que torna a solução como ponto único de falha.
- Dependência de renovações custosas de licenças.
- Exigência de técnicos especializados na Prefeitura ou a contratação de técnicos especializados terceiros.

3. Justificativa da Necessidade da Aquisição ou Contratação

Diante do cenário de ameaças cibernéticas em constante evolução, é imprescindível que a Prefeitura Municipal de Lajeado adote medidas robustas para salvaguardar suas informações sensíveis e garantir o adequado funcionamento de suas operações. Nesse sentido, a aquisição de uma solução de segurança integrada, moderna e eficiente é essencial para mitigar riscos, prevenir incidentes de segurança e assegurar a continuidade das atividades institucionais. Em razão desse cenário, a contratação de uma nova solução de segurança cibernética justifica-se pelos seguintes pontos:

- **Fim da Vigência do Contrato e Limitações Legais**
    - Os Contratos nº 037-04/2020 (firewall), nº 029-01/2021*9 (antivírus) e nº 72-01/2025 (segurança SECaaS) anteriormente firmados soluções de firewall e antivírus, mesmo após estendidos dentro das premissas legais, atualmente estão em fase de esgotamento.
    - A impossibilidade de nova prorrogação contratual exige a abertura de novo processo licitatório para assegurar a continuidade dos serviços de segurança.
- **Custos e Dependência de Suporte Especializado**
    - As **renovações anuais** de licenças e suporte tornam-se cada vez mais onerosas em função da desatualização do hardware.
    - Há dependência de **técnicos especializados** no ambiente de tecnologia da Prefeitura ou de serviços terceirizados para o suporte, implicando custos constantes para se manter a solução devidamente configurada e segura.
- **Benefícios de uma Solução mais Moderna e Flexível**
    - **Administração e monitoramento remoto** com possibilidade de reação imediata em regime **24x7x365**, reduzindo o tempo de resposta a incidentes e potencializando a proteção do ambiente.
    - **Recursos avançados** de detecção de ameaças, integrando tecnologias de inteligência artificial, sandboxing e inspeção profunda de pacotes (DPI), alinhadas às demandas atuais de segurança cibernética.
    - Maior **flexibilidade de contratação**, incluindo possíveis soluções em **modelo de serviço (SECaaS ou Security as a Service)** ou **appliance de última geração**, permitindo à Prefeitura optar pela modalidade que melhor se encaixa em seu planejamento orçamentário e operacional.
    - Implementação de **rotinas de pentest e hardening** constantes, garantindo que as configurações de segurança sejam testadas e endurecidas regularmente, de acordo com as melhores práticas de mercado.
    - Possibilidade de adoção de ambiente de **alta disponibilidade (HA ativo-ativo, ativo-passivo ou com programa de substituição imediato)**, eliminando ou mitigando o ponto único de falha e fortalecendo a resiliência dos serviços prestados.
- **Continuidade Operacional e Proteção Ampliada**
    - A aquisição de uma nova solução de firewall garante a **continuidade operacional** e a **proteção ininterrupta** da infraestrutura de TI, fundamentais

para os serviços da Prefeitura de Lajeado, evitando indisponibilidades e riscos de segurança.
    - A contratação atualizada permitirá o **alinhamento com as políticas e normas de segurança** mais recentes, contribuindo para a manutenção da conformidade legal e regulatória.

Diante de todos esses fatores, constata-se que a **contratação ou aquisição de uma nova solução de segurança como serviço** é medida necessária para assegurar a **eficácia na proteção do ambiente de rede**, manter a **continuidade dos serviços** prestados à população e garantir o **cumprimento das exigências legais** e de **boas práticas em segurança da informação**. Por meio de um novo processo licitatório, será possível avaliar o mercado, considerar soluções mais modernas, flexíveis e escaláveis, bem como viabilizar a adoção de recursos que forneçam monitoramento 24x7x365, alta disponibilidade, testes de intrusão e aprimoramento contínuo das políticas de segurança.

4. Requisitos da Contratação

A solução contratada deve incluir:

- Firewall de próxima geração (NGFW) com IDS/IPS e prevenção de ameaças de dia zero.
- Suporte a redes virtuais e ambientes híbridos.
- Gerenciamento centralizado com análise de logs.
- Contrato de suporte técnico 24x7x365 com SLAs pré-definidos.
- Atualizações regulares sem custos adicionais.
- Segurança de endpoints com adoção de antivírus corporativo (enterprise).

O objetivo deste projeto é implementar uma solução de segurança de ponta, contemplando firewall, antivírus e monitoramento em modalidade Software as a Service (SECaaS). A contratação de uma empresa especializada será fundamental para garantir a proteção dos ativos da organização, reduzindo riscos, atendendo a requisitos regulatórios e otimizando recursos. A seguir, são apresentados os principais pontos a serem considerados:

- **Escopo da Solução**
    - **Firewall de Próxima Geração (NGFW):** Capacidade de inspeção profunda de pacotes, bloqueio de ameaças avançadas e aplicação de políticas granulares de segurança.
    - **Serviços Gerenciados e Suporte:** Monitoramento proativo, relatórios regulares, suporte 24x7x365 e escalonamento rápido para incidentes de alta criticidade.
    - **Integração com Outros Serviços:** Compatibilidade com sistemas de monitoramento, soluções de endpoint e ferramentas de inteligência de ameaças (Threat Intelligence).
    - **Licenças de Antivírus**: Integração da plataforma de solução de antivírus com os demais serviços gerenciados de segurança, compondo um sistema holístico na segurança corporativa.
- **Modalidade SECaaS**

    - **Entrega pela Nuvem:** Disponibilização da solução como serviço, evitando custos elevados de hardware e manutenção on-premises.
    - **Atualizações Automáticas:** A empresa contratada deve garantir a atualização contínua de regras de segurança, patches e melhorias, sem interrupção significativa do serviço.
    - **Escalabilidade e Flexibilidade:** Possibilidade de ampliar ou reduzir recursos (largura de banda, filtros, módulos extras de segurança) conforme a necessidade, sem aquisição de novos equipamentos.
- **Novas Abordagens de Segurança**
    - **Modelo Zero Trust:** Segmentação da rede e verificação contínua de identidade e contexto, dificultando movimentos laterais de ameaças.
    - **Defesa em Profundidade:** Implementação de camadas múltiplas de segurança (filtro de conteúdo, sistemas de detecção de intrusão e controle de acesso).
    - **Machine Learning e Automação:** A solução proposta deve possuir recursos de IA/ML para detecção de anomalias e respostas automatizadas a incidentes.
- **SLA e Disponibilidade**
    - **Baixo SLA de Resposta a Incidentes:** O parceiro contratado deve atender rapidamente a ocorrências, garantindo baixo tempo de inatividade.
    - **Alta Disponibilidade (HA):** Redundância e failover automático, assegurando continuidade do serviço em caso de falha de um componente ou do provedor principal.
    - **Planos de Recuperação de Desastres (DR):** Garantia de retomada ágil das operações, com procedimentos documentados e testados regularmente.
- **Requisitos de Contratação**
    - **Critérios Técnicos:** Capacidade de lidar com volumetria de tráfego, latência reduzida e relatórios de auditoria conforme normas vigentes.
    - **Compliance e Certificações:** Avaliação das certificações do fornecedor (ISO 27001, SOC 2, PCI-DSS, entre outras), assegurando boas práticas de mercado.
    - **Equipe Especializada:** Expertise em configurações avançadas de firewall, monitoramento, segurança de rede, segurança de endpoints e metodologias de resposta a incidentes.
    - **Escopo de Serviços e Níveis de Suporte:** Clarificar responsabilidades do fornecedor, métricas de performance, tempo de resposta e de resolução de problemas.
    - **Custos e Modelos de Pagamento:** Transparência na precificação, contemplando escalabilidade, licenciamento e eventual expansão de funcionalidades.
- **Cronograma e Fases do Projeto**
    - **Planejamento e Análise:** Mapeamento de necessidades específicas da organização, definição de indicadores de performance e validação de requisitos técnicos.
    - **Implantação e Configuração:** Configuração inicial da solução, testes de desempenho e ajustes necessários para garantir aderência às políticas internas.

    - **Operação e Suporte:** Entrar em regime de operação com monitoramento constante, identificando pontos de melhoria ao longo do contrato.
    - **Avaliação Contínua:** Revisões periódicas de SLA, relatórios de incidentes e análise de vulnerabilidades para promover ajustes e melhorias graduais.
- **Resultados Esperados**
    - **Aperfeiçoamento da Postura de Segurança:** Redução drástica de ameaças e aumento da resiliência contra ataques cibernéticos.
    - **Melhoria no Cumprimento de Normas e Regulamentos:** Maior conformidade com leis de proteção de dados e padrões internacionais de segurança.
    - **Escalabilidade e Sustentabilidade:** Capacidade de crescimento seguro do ambiente sem demandar grandes investimentos em infraestrutura própria.
    - **Otimização de Custos e Recursos:** Redução de gastos e sobrecarga operacional, uma vez que as atividades de suporte e manutenção ficam a cargo da empresa contratada.

Em conclusão, a adoção de uma solução de segurança em modalidade SECaaS, somada às boas práticas nas áreas de Redes de Computadores, Dispositivos Pessoais, Acesso à Internet e Segurança da Informação possibilitará uma operação mais eficiente, segura e escalável. É essencial escolher uma solução que ofereça recursos avançados de detecção, mitigação de ameaças e suporte especializado assegurando, pelo menos, os princípios de Confidencialidade, Integridade e Disponibilidade das operações administrativas e dos serviços públicos, mesmo em cenários de alta criticidade.

5. Levantamento das Soluções Existentes e Viabilidade

Solução 1: Compra do equipamento e das assinaturas dos serviços na modalidade *on premise* (CAPEX)

Viabilidade de Mercado

A aquisição de equipamentos e assinaturas de serviços on premise continua sendo uma opção amplamente oferecida pelo mercado de tecnologia, uma vez que diversos fornecedores e integradores disponibilizam soluções para armazenamento, processamento e gerenciamento de dados em instalações próprias. Essa modalidade é atrativa para organizações que desejam maior controle de hardware, segurança mais customizável e eventuais requisitos específicos de regulamentação.

- **Atratividade**: Em função da diversidade de fornecedores, há concorrência suficiente para buscar condições comerciais vantajosas.
- **Acompanhamento de tendências**: Apesar do avanço de soluções em nuvem, o mercado de tecnologias on premise permanece ativo para atender nichos que requerem infraestrutura interna, garantindo a existência de suporte e atualizações.

Viabilidade Econômica

A compra dos equipamentos implica em um investimento inicial elevado, incluindo custos de aquisição de servidores, sistemas de armazenamento e dispositivos de rede, além de licenças de software para operacionalização.

- **Custo de capital (CAPEX)**: O projeto demandaria uma alocação significativa de recursos financeiros no momento inicial. Conforme apontado nos textos do Projeto TI, há necessidade de justificar esse desembolso em função da vida útil dos equipamentos e do retorno esperado.
- **Custos de manutenção e atualização**: Manter a infraestrutura atualizada e corrigir eventuais falhas exige um orçamento contínuo, pois componentes de hardware podem exigir substituição e softwares precisam de licenças anuais de suporte.
- **Escalabilidade**: Caso haja crescimento acelerado do volume de dados ou da demanda por serviços, novos gastos em aquisição de hardware poderão onerar substancialmente o orçamento ao longo do tempo.

Viabilidade Operacional

A infraestrutura adquirida demandará equipes internas de TI capacitadas para instalação, configuração, monitoramento e suporte contínuo.

- **Recursos humanos e competências**: A manutenção de equipe especializada é fundamental para lidar com a complexidade do ambiente e eventuais incidentes.
- **Controle e segurança**: O controle sobre todo o parque tecnológico e a política de segurança fica concentrado na organização, permitindo personalizações avançadas. Em contrapartida, a responsabilidade integral pela segurança e conformidade regulatória recai sobre a equipe interna.
- **Tempo de implementação**: A configuração e implantação podem ser mais demoradas, haja vista o processo de compra, entrega e preparação da infraestrutura. Ainda assim, essa modalidade pode ser considerada robusta e confiável, desde que devidamente planejada.

Solução 2: Solução na modalidade SECaaS (SECURITY AS A SERVICE) para serviços e hardwares (OPEX)

Viabilidade de Mercado

A adoção de SECaaS (Security as a Service) em conjunto com hardware em comodato, no qual o fornecedor se responsabiliza pela disponibilidade dos equipamentos, softwares, middleware e serviços, é uma tendência crescente no mercado de tecnologia. Organizações buscam cada vez mais a redução de custos iniciais e a flexibilidade de escalabilidade, tornando esse formato de aquisição e utilização de serviços bastante difundido.

- **Parcerias estratégicas**: Os principais fabricantes e provedores de serviço vêm expandindo seus modelos de negócios para contemplar comodato, em linha com a demanda de clientes que preferem evitar imobilização de capital em infraestrutura.
- **Facilidade de adoção**: Pelo fato de o fornecedor cuidar da maior parte da infraestrutura, a curva de adoção tende a ser mais simplificada, reduzindo o tempo de implementação.

Viabilidade Econômica

No modelo SECaaS com comodato, os investimentos em hardware são diluídos em mensalidades ou assinaturas, reduzindo o desembolso inicial de capital.

- **OPEX em vez de CAPEX**: Transforma boa parte dos gastos em despesas operacionais, facilitando a previsão orçamentária e o fluxo de caixa.
- **Custo total de propriedade (TCO)**: Se por um lado o custo recorrente pode se somar ao longo dos anos, por outro, elimina-se a necessidade de despesas de atualização e manutenção de hardware, uma vez que tais custos são absorvidos em grande parte pelo fornecedor.
- **Escalabilidade econômica**: O modelo permite ajustar os recursos conforme a necessidade, reduzindo riscos de subutilização ou superdimensionamento da infraestrutura.

Viabilidade Operacional

Com a maior parte dos serviços sendo provida em SECaaS, a equipe de TI interna foca principalmente na governança, gestão dos contratos e monitoramento dos SLAs (Service Level Agreements).

- **Responsabilidade compartilhada**: O fornecedor se responsabiliza pela disponibilidade do ambiente e manutenção dos equipamentos em comodato, enquanto a organização zela pela correta configuração, segurança dos dados e compliance com a legislação.
- **Agilidade de implantação**: O tempo de implementação tende a ser menor em comparação a um ambiente totalmente on premise, pois hardware e software já estão pré-configurados e gerenciados pelo fornecedor.
- **Dependência de terceiros**: Apesar das vantagens operacionais, a instituição fica mais dependente do fornecedor para suporte e resolução de incidentes, devendo estabelecer acordos contratuais robustos para assegurar continuidade e desempenho do serviço.

Solução 3: Aquisição de Ativos (CAPEX) com Contratação de Serviços de Operação e Monitoramento 24x7 (OPEX)

Viabilidade de Mercado

- **Domínio do Ativo:** O mercado ainda oferece a venda de hardware (*appliances* de Firewall), permitindo que a prefeitura detenha o patrimônio físico. É uma modalidade comum em órgãos que possuem dotação orçamentária específica para investimentos (Despesas de Capital).
- **Ecossistema de Parceiros:** Existem diversos integradores capazes de operar hardwares de terceiros, garantindo que a prefeitura não fique "presa" ao fabricante para a operação do dia a dia.
- **Desafio de Atualização:** O mercado de segurança evolui rápido; a compra do hardware exige que o edital preveja a atualização de assinaturas (licenciamento) vinculada ao serviço, caso contrário, o equipamento torna-se um "peso de papel" digital.

Viabilidade Econômica

- **Investimento Inicial Elevado (CAPEX):** Exige um desembolso vultoso no início do contrato para a compra dos equipamentos (Classificação: Despesas de Capital / Material Permanente).
- **Custo de Manutenção (OPEX):** Reduz o valor mensal em comparação ao SECaaS puro, pois a prefeitura já é dona do hardware. O pagamento mensal foca exclusivamente no serviço de monitoramento 24x7 (SOC - Security Operations Center) e suporte técnico.
- **Depreciação Patrimonial:** Economicamente, o ativo perde valor e eficácia técnica em média após 60 meses, exigindo um novo ciclo de investimento (CAPEX) ao fim do período.

Viabilidade Operacional

- **Gestão Híbrida:** A prefeitura detém o controle físico do ambiente (dentro do seu datacenter), mas transfere a responsabilidade da configuração e monitoramento 24x7 para uma empresa especializada.
- **Riscos de Hardware:** Caso o equipamento apresente defeito físico após a garantia, o ônus da substituição e o tempo de indisponibilidade recaem sobre o processo de reposição da prefeitura, a menos que o contrato de serviço preveja *NBD (Next Business Day)* para peças.
- **Monitoramento 24x7:** Garante que, embora o equipamento seja próprio, a vigilância contra ataques ocorra ininterruptamente por especialistas externos.

Conclusão do Levantamento e Justificativa (Comparativo Atualizado)

Considerando o diagnóstico e as diretrizes estratégicas delineadas nos documentos já produzidos para o Projeto TI, cada solução apresenta vantagens e riscos específicos. A Solução 1 (on premise) é tradicional e confere maior controle, mas demanda alto investimento inicial e maior responsabilidade de manutenção. A Solução 2 (SECaaS + comodato) alinha-se às tendências de mercado, reduz investimentos iniciais e torna a operação mais ágil, porém aumenta a dependência de terceiros. Já a Solução 3 (manter a solução atual) adia custos imediatos, mas pode acarretar em riscos crescentes de obsolescência e prejuízos à continuidade do serviço. Considera-se ainda:

- **Solução 1 (On-Premise Clássico):** Maior controle, porém exige equipe interna altamente especializada e alto investimento inicial.
- **Solução 2 (SECaaS):** Maior agilidade e atualização tecnológica automática. Baixo investimento inicial, transformando tudo em custo fixo mensal (OPEX). Ideal para orçamentos de custeio.
- **Solução 3 (Misto: Compra + Serviço):** Permite a incorporação de patrimônio (CAPEX), porém adiciona o custo mensal de serviço e mantém o risco de obsolescência do hardware sob responsabilidade da prefeitura e exige gestão de ativos.

6. Análise e Comparação das Soluções Existentes e Justificativa da Solução Eleita

Para subsidiar a decisão acerca da melhor estratégia de implementação, foi realizada uma avaliação criteriosa de três possíveis soluções, com base nos aspectos de vantajosidade, economicidade, adaptabilidade, escalabilidade, eficiência, simplicidade, custos operacionais e compatibilidade com as tendências na administração pública. A seguir, descrevem-se os principais pontos observados e a justificativa para eleger a **Solução 2** como a opção mais adequada.

Vantajosidade e Economicidade

- **Solução 1**:
  Apresenta custo inicial relativamente elevado em razão de investimentos em infraestrutura dedicada e licenças específicas. Embora possa oferecer certas funcionalidades de alto desempenho, a relação custo-benefício tende a ser menos atrativa ao longo do ciclo de vida, sobretudo por demandar constantes atualizações e manutenção especializada.
- **Solução 2**:
  Equilibra investimentos iniciais e custos de manutenção ao longo do tempo, empregando recursos tecnológicos amplamente suportados no mercado. Esse modelo possibilita reduções significativas em licenças e treinamentos, favorecendo uma adoção menos onerosa no curto prazo e melhor previsibilidade orçamentária no médio e longo prazo.
- **Solução 3**:
  Apesar de exigir menor custo inicial quando comparada à Solução 1, suas funcionalidades são mais limitadas, especialmente em termos de suporte técnico e disponibilidade de módulos específicos. Essa limitação implica uma possível elevação de custos em eventuais customizações para atender demandas futuras.

Adaptabilidade

- **Solução 1**:
  Oferece certas possibilidades de customização, mas a complexidade de desenvolvimento e implantação de novos módulos pode prolongar prazos de entrega. Assim, adaptações a novos requisitos ou regulamentações podem demandar esforços técnicos adicionais.
- **Solução 2**:
  Apresenta arquitetura modular e flexível, o que facilita a realização de ajustes e expansões conforme surjam novas demandas ou mudanças regulatórias. Possibilita incorporar inovações tecnológicas sem causar interrupções significativas às operações rotineiras.
- **Solução 3**:
  Baseia-se em uma estrutura pré-definida, com menor margem de customização. Ainda que atenda a requisitos básicos iniciais, a falta de modularidade pode dificultar

a incorporação de melhorias ou adaptações futuras, tornando-a menos eficiente para projetos de maior porte ou em constante evolução.

Escalabilidade

- **Solução 1**:
  A ampliação da capacidade de processamento ou armazenamento exige investimentos substanciais em infraestrutura proprietária. Essa característica onera o processo de expansão e limita a adaptação a picos de demanda.
- **Solução 2**:
  Desenvolvida sobre fundamentos que permitem utilizar recursos de forma gradativa, potencializando o uso de plataformas em nuvem ou soluções de microserviços. Essas práticas viabilizam a escalabilidade conforme o crescimento das necessidades institucionais, mantendo o controle de custos.
- **Solução 3**:
  Mostra-se adequada para uma adoção inicial mais simples; porém, a falta de planejamento para crescimento e a estrutura de suporte ainda pouco robusta podem prejudicar seu desempenho caso haja aumento expressivo de usuários ou de volume de processamento.

Eficiência e Simplicidade

- **Solução 1**:
  Embora tenha diversas funcionalidades avançadas, exige uma curva de aprendizado prolongada e processos de suporte mais complexos. Consequentemente, a operacionalização inicial pode demandar treinamentos intensivos e maior envolvimento de equipes técnicas.
- **Solução 2**:
  Propõe fluxos de trabalho simples e componentes modulares, o que favorece a adoção por usuários com diferentes perfis e reduz a dependência de suporte especializado. Essa abordagem otimiza a produtividade e facilita o alinhamento entre equipes técnicas e de negócio.
- **Solução 3**:
  Apresenta uma interface de uso relativamente simples em seu estado padrão. Contudo, quando surge a necessidade de recursos mais complexos, o sistema pode se tornar menos intuitivo, dificultando a adoção de boas práticas de governança e controle. Além disso, necessita possuir equipe especializada interna ou depender de contratação específica.

Custos Operacionais

- **Solução 1**:
  Os custos de manutenção incluem despesas regulares com licenciamento, suporte especializado e atualizações. Em longo prazo, a soma desses elementos pode comprometer o orçamento e dificultar a gestão financeira do projeto.
- **Solução 2**:
  Traz maior previsibilidade e flexibilidade nos custos, uma vez que a manutenção e o suporte podem ser terceirizados ou pactuados em contratos de serviço sob

demanda. Dessa forma, torna-se mais ágil adequar o orçamento e otimizar recursos ao longo do tempo.

- **Solução 3**:
  Embora tenha custos iniciais menores, a ausência de um ecossistema robusto de suporte e a necessidade de customizações externas podem resultar em elevações inesperadas no orçamento operacional, especialmente para atender requisitos mais complexos.

Compatibilidade com as Tendências na Administração Pública

- **Solução 1**:
  Atende a diversos requisitos de segurança e compliance, mas sua arquitetura pouco flexível pode não acompanhar facilmente iniciativas de transformação digital e interoperabilidade em âmbito governamental.
- **Solução 2**:
  Compatível com as tendências de modernização e digitalização, pois prioriza padrões abertos e integra-se com outros sistemas públicos de maneira fluida. Essa aderência favorece a transparência, a governança de dados e a adoção de boas práticas tecnológicas no setor público.
- **Solução 3**:
  Embora contemple funcionalidades básicas, não apresenta um histórico sólido de integrações amplas na administração pública. Isso pode exigir esforço adicional para adequar-se às políticas de interoperabilidade governamentais e exigências de segurança.

Justificativa da Solução Eleita

Após a avaliação técnica, financeira e estratégica das três alternativas, a **Solução 2** evidencia-se como a mais equilibrada e vantajosa. No caso de Segurança da Informação, comprar um hardware que ficará obsoleto em 5 ou seis anos (CAPEX) pode ser considerado ineficiente. Alugar o serviço com garantia de atualização tecnológica (OPEX) alinha-se melhor ao interesse público de manter a rede sempre protegida contra novas ameaças. O "Custo Total de Propriedade" (TCO) do serviço (OPEX) normalmente se mostra mais vantajoso ao longo de 5 anos, tempo previsto de contratação e prorrogável por mais 5 anos.

Essa escolha justifica-se pela capacidade de garantir:

- **Economia de recursos** e melhor relação custo-benefício, assegurando sustentação orçamentária contínua;
- **Adaptabilidade** a novos requisitos ou mudanças regulatórias, favorecendo a perenidade do projeto;
- **Escalabilidade** para atender a futuras demandas, com menor impacto em infraestrutura e maior eficiência;
- **Simplicidade operacional**, otimizando a rotina administrativa e reduzindo a necessidade de suporte intensivo;

- **Alinhamento às políticas de modernização e transparência** vigentes na administração pública, bem como integração com sistemas já existentes e aderência a padrões abertos.

Em síntese, a Solução 2 agrega os fatores cruciais para o sucesso do projeto no longo prazo, assegurando conformidade, eficiência e excelência no atendimento às demandas do setor público.

Considerando o Art. 18, §1º, da Lei 14.133, opta-se pelo modelo de prestação de serviço (Despesa Corrente) para garantir a atualização tecnológica contínua e evitar a obsolescência precoce do ativo, garantindo maior eficiência ao erário.

A Lei nº 14.133/2021 (Nova Lei de Licitações) não utiliza o termo "OPEX" explicitamente, pois essa é uma nomenclatura do mercado financeiro e privado. No entanto, ela favorece e incentiva o modelo de serviço (Despesas Correntes) em detrimento da compra de ativos (Despesas de Capital), especialmente em Tecnologia da Informação (TI).

Não há uma "imposição", mas existem diretrizes e mecanismos dentro da lei que tornam a OPEX a escolha tecnicamente mais adequada aos princípios da economicidade, planejamento, eficácia e celeridade.

7. Descrição Detalhada do Produto e/ou Serviço

A escolha adequada de uma solução de segurança corporativa que envolve tanto os acessos WEB quanto os endpoints (Dispositivos de uso pessoal) é fundamental para garantir que a Prefeitura Municipal de Lajeado esteja alinhada às melhores práticas de segurança da informação, bem como às normas e regulamentações vigentes. Ao adotar uma abordagem abrangente e proativa, a Prefeitura Municipal de Lajeado reafirma seu compromisso em proteger os dados e a privacidade dos cidadãos, promovendo a confiança e a transparência em suas operações. Para tanto, segue a descrição da solução pretendida.

7.1 CARACTERÍSTICAS GERAIS DO FIREWALL

Funcionalidades de NGFW (Next Generation Firewall) com reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões. Para proteção do ambiente, o dispositivo deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos) integrados ao próprio appliance, além de ser otimizado para análise de conteúdo de aplicações em camada 7.

O firewall deve ser fornecido no formato “appliance”, definido como um equipamento que dispõe de processamento, memória e demais recursos tecnológicos dedicados a um determinado serviço, projetado para executar tarefas de forma eficiente e simplificada, com recursos e software otimizados. Não se aceitam soluções baseadas em computadores de uso geral (PCs ou servidores) nem soluções que combinem hardware e software de fabricantes distintos.

Os firewalls devem ser entregues com licenciamento válido por no mínimo 60 (sessenta) meses, incluindo garantia e suporte e devem ser capazes de atualizar automaticamente firmware, patches e atualizações de segurança. A solução precisa permitir uso de armazenamento externo para System Logs, Threat Logs, AppFlow reporting data e Packet Captures, garantindo persistência de dados após reinicializações.

O painel de gerenciamento deve exibir o último contato do firewall com o gerenciador de licenciamento, bem como o status de atualizações de licenças e assinaturas. Deve também fornecer APIs para que fornecedores externos de NAC possam transmitir contexto de segurança aos firewalls, possibilitando a utilização simultânea de vários fabricantes. Por fim, não pode haver exceções de inspeção de tráfego (bypass) aplicadas automaticamente devido à limitação de capacidade de processamento. Qualquer exceção deve ser autorizada explicitamente por meio de documento oficial pelo fiscal do contrato.

7.1.2 Requisitos mínimos do firewall

Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 9.5 Gbps ou superior.
Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 4 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.
Desempenho mínimo de 10 Gbps de IPS.
Suporte mínimo de 4.000.000 conexões simultâneas/concorrentes no modo SPI.
Suporte mínimo de 115.000 novas conexões por segundo.
Deve possuir armazenamento interno de no minimo 128 GB e suportar expansão de armazenamento interno para até 1TB.
Deve possuir fonte de alimentação HotSwap com chaveamento automático de 100-240 VAC.
Deve possuir uma fonte de alimentação "HotSwap" redundante
Deve possuir 24 interfaces 1 GbE padrão RJ-45.
Deve possuir pelo menos 4 interfaces 10GbE SFP+;
Deve possuir 1 interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.
Deve possuir 2 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.
A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 500 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 3000 usuários simultâneos.
A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1000 usuários simultâneos.
Deve suportar 3800 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.
Deve suportar, no mínimo, 10 Gbps de desempenho de VPN IPSEC.
Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. 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.
O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.
O Equipamento deverá ser homologado pela ANATEL.
Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.
O licenciamento para todos os serviços de Next Generation Firewall deverá ser de, no mínimo, 60 meses.
A garantia do hardware deverá ser de 60 meses.
O equipamento deverá ser do tipo **rack-mount** (montável em rack), com dimensões físicas compatíveis com a instalação em gabinetes padrão de 19 polegadas, e ser fornecido com todos os acessórios, suportes e trilhos necessários para a sua fixação
O equipamento deverá ser do tipo rack-mount (montável em rack), com altura máxima de 1U (uma unidade de rack) e dimensões físicas compatíveis com a instalação em gabinetes padrão de 19 polegadas. O equipamento deve ser fornecido com todos os acessórios, suportes e trilhos necessários para a sua fixação.

7.2 CARACTERÍSTICAS DIVERSAS DO FIREWALL

Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.
Para proteção do ambiente contra ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Antispyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.
A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.
Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade.
Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.
Os firewalls devem ser entregues com licenciamento válido para, no mínimo, 60 (sessenta) meses, incluindo garantia e suporte.
Deve ser capaz de atualizar de forma automática o Firmware, patches e atualizações de segurança.
A solução deve permitir o uso de armazenamento externo para System Logs, Threat Logs, AppFlow reporting data e Packet Captures, garantindo persistência de dados após reinicializações do firewall
O painel deve exibir detalhes sobre o último contato do Firewall com o gerenciador de licenciamento, mostrando o status de atualização de licenças e atualizações de assinaturas
Deve fornecer APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança aos firewalls e que esta funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos.

A solução de segurança não pode aplicar nenhum tipo de exceção de inspeção de tráfego (bypass) oriunda de condições de limitação de capacidade de processamento de forma automática. Toda e qualquer exceção (bypass) de inspeção e tráfego deve ser possível apenas através de ação explícita e específica criada pelo administrador da plataforma através de configurações realizadas pela console gráfica do appliance, ou pela plataforma centralizada de gerenciamento da solução.
Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.
Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do túnel IPSec.
Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
Deve possuir proteção anti-spoofing.
Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;
Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.
Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado: endereço de origem, endereço de destino, serviço e aplicação.
Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:
Baixa Latência;
O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal lógico.
A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.
A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.
Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.
Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.
Deve suportar DHCP relay.
Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.
Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (fisica e virtual) ou zona de segurança.
Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em

grupo.
Deve ter suporte a proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.
Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.
Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.
Detectar e bloquear a origem de port scans.
Deve permitir o bloqueio de ataques.
Deve permitir o bloqueio de exploits conhecidos.
O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP, e SMTP.
Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser decriptografado de forma transparente à aplicação.
Implementar DSCP (Differentiated Services Code Points).
Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.
Implementar controle e gerenciamento de banda para a tecnologia VoIP(Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.
Implementar mecanismo de sincronismo de horário através do protocolo NTP.
Possuir suporte ao protocolo SNMP versões 2 e 3.
Possuir suporte a log via syslog.
Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.
Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.
Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.
Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.2 e TLS 1.3
Deve permitir a funcionalidade de ARP bridging
Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm"
A solução deve permitir a visualização gráfica das regras de segurança e acesso.
O equipamento deverá prover a funcionalidade de servidor NTP (Network Time Protocol) para sincronização precisa de data e hora dos dispositivos da rede

Para os modelos de firewall que porventura sejam entregues com funcionalidade wireless, o equipamento deverá suportar os padrões de segurança WPA2/WPA3 Enterprise e protocolo de autenticação EAP em modo estação, oferecendo maior proteção para as conexões sem fio
O firewall deverá implementar a funcionalidade de DNS proxy para otimizar e controlar as requisições de resolução de nomes de domínio na rede
CARACTERÍSTICAS DE VPN
Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.
Suportar algoritmos de criptografia 3DES, AES 128, AES 256 e AESGCM16-256
Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.
Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.
Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.
Autenticação via túneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.
A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.
Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.
Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.
A solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.
Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.
Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.
Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.
Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.
Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.
Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
CONTROLE DE AMEAÇAS
Para as ameaças de dia zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.
A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.
Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.
Implementar funcionalidade de detecção e bloqueio de “call-backs”.

A solução deverá ser capaz de detectar e bloquear comportamentos suspeitos ou anormais da rede.
A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.
Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.
Implementar interface CLI segura através do protocolo SSH.
Possuir Antivírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.
A solução deve permitir criar regras de exceção de acordo com a proteção.
Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;
Permitir o bloqueio de malwares (vírus, worms, spyware e etc).
A solução deve ser capaz de proteger contra ataques a DNS.
A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.
A solução deve ser capaz de prevenir acesso a websites maliciosos.
A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.
A solução deverá receber atualizações de um serviço baseado em cloud.
A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.
A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.
A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade
A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente às ameaças exploradas por vulnerabilidades do tipo meltdown .
A solução de Gateway AntiVírus deverá ter a tecnologia complementar de Antivírus-Cloud, para que os mecanismos existentes de verificação sejam ampliados.
A solução deve bloquear proativamente o acesso a domínios maliciosos conhecidos por meio de filtragem DNS, reduzindo assim o risco de infecções por malware e outros ataques cibernéticos.
A solução deve prover o bloqueio de URL baseado em reputação, identificando e bloqueando proativamente entidades suspeitas.
PROTEÇÃO CONTRA ATAQUES AVANÇADOS
A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.
Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.
A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.
Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.
Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.
Implementar detecção e bloqueio imediato de malwares que utilizam mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivos

PDF com até 10Mb.
Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.
Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.
A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.
A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliances através de assinaturas.
Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.
Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;
Conter ameaças avançadas de dia zero.
Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador.
Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;
Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.
Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.
Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.
Possuir Antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP , IMAP e CIFS.
Mitigar ameaças de dia zero de forma transparente para o usuário final.
Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.
Implementar mecanismo de pesquisa por diferentes intervalos de tempo.
Mitigar Ameaças de dia zero via tráfego de internet.
Permitir a contenção de ameaças de dia zero sem a alteração da infra-estrutura de segurança.
Mitigar Ameaças de dia zero que possam burlar o sistema operacional emulado.
A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.
Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.
Conter e mitigar exploits avançados.
A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Antivírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede).
Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.
As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real.

A Solução de segurança de FireWalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or buffering.
A Solução deve unificar diversas funções de segurança em um único conjunto integrado, inspecionando os arquivos de usuários locais, remotos e móveis.
A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS, etc., sem afetar o desempenho.
A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças , com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:
Inspeção profunda de memória em tempo real
Descriptografia e inspeção TLS/SSL,
Inteligência e controle de aplicativos
Recursos SD-WAN seguros
CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB
Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 89 (oitenta e nove) categorias distintas, com mecanismo de atualização e consulta automáticas.
Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, Active Directory e base de dados local
Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.
Permitir a customização de página de bloqueio.
Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.
Deve permitir submissão de novos sites para categorização.
Permitir a classificação dinâmica de sites web, URLs e domínios.
Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.
Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.
Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.
CARACTERÍSTICAS DE AUTENTICAÇÃO
Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.
Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs +, Single Sign On e API.
Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.
Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais

devem ser obtidos automaticamente pelo NGFW.
Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.
Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW.
Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.
Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.
Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet
A solução deve possibilitar SSO via API
O firewall deverá suportar autenticação SSO via SAML 2.0 (Security Assertion Markup Language) para integração com provedores de identidade em nuvem, garantindo compatibilidade com ao menos Azure AD/Entra ID, Google Workspace/G Suite e Okta.
CARACTERÍSTICAS DE ADMINISTRAÇÃO E RELATÓRIOS
Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.
Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.
Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.
Possuir mecanismo para agendamento e realização das cópias de segurança(backups) de configuração.
Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.
A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.
Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões.
Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.
Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.
Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de “ICMP Unreachable” para máquina de origem do tráfego, “TCP-Reset” para o cliente, “TCP-Reset” para o servidor ou para os dois lados da conexão.
Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.
Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.
Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6.
Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.
Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML e CSV: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).
Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.
Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.
A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.
O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.
O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.
O aplicativo móvel deve permitir a visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.
O aplicativo móvel deve permitir a visualização dos últimos logs gerados no NGFW.
O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.
O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.
A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto-provisionamento da plataforma através de ponto central de gerenciamento.
Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações
A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas.
Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful
Deve possuir solução de gerenciamento centralizado de toda a solução de firewall.
Deve permitir o controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções
Deve dar suporte a organização os dispositivos administrados por grupos;
Deve ser possível aplicar configurações de forma granular, um um firewall, em grupos, ou em todos os firewalls.
Deve mostrar os status dos firewalls (standalone ou em alta disponibilidade) a partir da plataforma de gerenciamento centralizado;

Centralizar a administração de regras e políticas usando uma única interface de gerenciamento;
O gerenciamento deve permitir/possuir:
Criação e administração de políticas de firewall e controle de aplicação
Monitoração de logs;
Debugging
Deve permitir acesso concorrente de administradores
Deve permitir o provisionamento de configuração por "Zero-Toutch"
A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL
O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados.
A solução deve possuir tela situacional com todo os inventários de firewalls gerenciados centralizadamente, informando no mínimo para o administrador, nome do Hostname do firewall, número de série, modelo, versão do firmware e status da conectividade do equipamento com a gerência em online ou off-line.
Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez;
Deve centralizar a administração de regras e políticas, usando uma única interface de gerenciamento;
A solução deve possuir Dashboard com sumário de alertas e informação de status de licença
A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo
Deve manter um canal de comunicação segura, com encriptação baseada HTTPS, entre todos os componentes que fazem parte da solução de firewall, gerência
A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão na console de gerência local do firewall sem a necessidade do administrador utilizar endereço IP do dispositivo, URL ou FQDN
A solução deve permitir a criação de modelos de configuração ou “Templates” para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls
Os modelos de configuração ou “templates” devem suportar configurações de interfaces físicas ou virtuais
A solução deve permitir a criação de grupos lógicos, para o agrupamento de dispositivos, com isso permitindo a aplicação de modelos de configuração a diversos equipamentos de uma única vez.
Deverá permitir visualizar a diferença nas mudanças antes que as configurações sejam implantadas.

De forma centralizada deve permitir gerenciar, mas não limitado há, políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configuração de endereçamento IP das interfaces dos equipamentos, criação e administração de políticas de IPS, configuração de políticas de antivírus e antimalware, configuração e criação de políticas de controle de URL, criação e configuração de políticas de controle de aplicações, criação e configuração de política de SANDBOX, criação e configuração de políticas de controle de banda, criação e configuração de objetos necessários para configuração das políticas especificadas acima, usando uma única interface de gerenciamento;
Deverá possibilitar a criação de políticas SD-WAN, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall.
Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria.
Durante a alteração de políticas de segurança dos firewalls, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente.
Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, esse processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente
A funcionalidade de Workflow deve permitir configurar, em dias, a validade dos pedidos de aprovação, caso o pedido de aprovação não seja aprovado no período configurado, essa mudança deve ser expirada e não efetivada.
A plataforma deve oferecer possibilidade de aplicação de senhas fortes por padrão, a critério do administrador da plataforma, e incluir mecanismos que desabilitem login quando identificados padrões de ataque de força bruta que visem comprometer credenciais de acesso ao dispositivo. Neste cenário, a plataforma deve ter a capacidade de invalidar senhas que possam potencialmente ter sido comprometidas, eliminando este vetor de ataque localmente e protegendo o dispositivo imediatamente

7.3 CARACTERÍSTICAS MÍNIMAS DO ANTIVÍRUS (EndPoint)

O produto deve ser uma plataforma integrada de gerenciamento de segurança modular que rode em uma infraestrutura virtualizada. O produto deve incluir os seguintes módulos:

a) Console de Gerenciamento fornecendo funcionalidades de Gestão;

b) Módulos para estações físicas, laptops e servidores.

c) Módulo para ambientes virtualizados. Um produto Anti Malware criado especialmente para ambientes virtuais.

d) Módulo para dispositivos móveis que provê segurança e controle de conformidade para Smartphones e tablets para sistemas operacionais iOS e Android.

7.4 REQUISITOS MÍNIMOS DO ANTIVÍRUS

CARACTERÍSTICAS GERAIS
Licenciamento básico com chave unitária com número global de usuários.
Arquitetura simples de atualização – bastando clicar em um botão “update” e todas as funções e serviços serão atualizados com os pacotes necessários.
Atualização de pacotes “On-demand” permite que o administrador escolha qual pacote será atualizado para conservar a banda.
Notificações – Sempre mostrar no menu principal, destacado como item não lido, enviar por email, alertar o administrador de problemas principais: problemas com licenças, alertas de surto de vírus, máquinas desatualizadas, eventos de antimalware
PAINEL DE MONITORAMENTO
Baseado em “portlets” configuráveis, onde pode especificar o nome, tipo de relatório, alvo do relatório, e opções específica para cada tipo de relatório (ex: para relatório de atualização – que é o intervalo de atualização para que o computador seja considerado desatualizado).operacional e endereço de IP.
“Portlets” disponíveis para qualquer serviço de segurança: Máquinas físicas, Máquinas virtuais, dispositivos móveis, servidores de email Exchange.
Suportando adição, remoção e reajustando a ordem.
GERENCIAMENTO DE SEGURANÇA
Integração com múltiplos domínios do Active Directory Domains, múltiplos VMware, vCenters, múltiplos Citrix Xen Servers e importação dos inventários dessas plataformas. Para a sincronização com o Active Directory, o administrador pode definir o intervalo da sincronização (em horas).
Compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. Para essas plataformas de virtualização, máquinas virtuais podem ser descobertas e listadas no console de gerenciamento via Descoberta de rede.
Descoberta de rede para máquinas em grupo de trabalho.
Busca em tempo real, ordenação e filtro por nome, Sistema operacional e endereço de IP.
Instalação remota e desinstalação do antivírus.
Instalação manual e configurável de pacotes de instalação antivírus.
Tarefas de Scan remote configuráveis.
Tarefa de reinicialização remota de uma estação ou servidor.
Resultados de tarefas centralizadas com detalhamento de cada subtarefa.
Assinar políticas para todos os níveis: computador, máquina virtual, OU, computer, virtual machine, OU, pastas.
Opção de assinar políticas poderosas: configurar herança de política, forçar políticas de configuração, etc.
Propriedades detalhadas de objetos gerenciados: Nome, IP, Sistema operacional, Grupo, Política Assinada, último status de malware, últimos logs de Scan.

POLÍTICAS
Modelo único para máquinas físicas e virtuais.
Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar e configurar as funcionalidades como escaneamento do Antimalware, firewall de duas vias com detecção de intrusão, controle de acesso à rede, controle de aplicação, controle de acesso web, criptografia, localização de dispositivo, aplicação de autenticação e ações para serem aplicadas em caso de malware e dispositivos em não conformidade, como travar remotamente, destravar, limpar
RELATÓRIOS
Relatórios para cada serviço de segurança.
Facilidade de usar em apenas uma visualização: Sumário e detalhes na mesma página, sessão de sumário ativo (filtros detalhados clicando na sessão sumário).
Agendamento, pode ser enviado por email para qualquer destinatário (Não é necessário ter uma conta no console).
Filtros para agendamento de relatórios para receber por email somente informações relevantes de cada usuário.
Arquivo com todas as instâncias de relatórios agendados.
Exportar o sumário para pdf e detalhes para csv.
Fornecer painéis digitais para acompanhamento de eventos.
PROTEÇÃO DE HOSTS
Métodos de detecção de vírus, spyware, rootkits, e outros mecanismos de segurança.
O produto deve permitir atualização automática do appliance virtual de segurança, para assinaturas de Antimalware e para o Sistema operacional do virtual appliance.
O produto deve reportar o estado atual do host de segurança – VMs protegidas/não protegidas e os appliances virtuais de segurança.
Plataformas de Virtualização a serem suportadas: VMware, Citrix, XenServer, Microsoft Hyper-V e Oracle VM 3.0

7.9 A solução SECaaS a ser contratada deve incluir:

- **Fornecimento de hardware e software** de acordo com o cenário atual da contratante, prevendo crescimento de, no mínimo, 33% nos primeiros 5 anos;
- **Licenciamento de solução de Antivírus (Endpoint Security)**, incluindo console de gerência centralizada (local ou nuvem), proteção contra malware, ransomware e proteção web;
- **Gestão de licenciamentos e atualizações** contínuas de softwares e assinaturas de segurança (vacinas e motores);
- **Monitoramento ativo 24x7x365** com respostas proativas a incidentes e ameaças em tempo real;
- **Inclusão e manutenção de regras**, políticas de segurança e filtros de conteúdo;

- **Hardening constante** dos ativos de rede e estações de trabalho para redução de vulnerabilidades;
- **Treinamento especializado** para a equipe interna quanto à operação e melhores práticas da solução;
- **Pentest de firewall anual** para validação da integridade do perímetro.

SLA

Para uma abordagem de segurança mais completa a solução vencedora deverá atuar com diversos processos em paralelo, com o objetivo de identificar, proteger, detectar, responder a ameaças de forma rápida e em conformidade com o Acordo de Nível de Serviço (SLA).

Assim que um incidente é identificado, responsáveis designados devem atuar sobre a ameaça e nos tempos estipulados no SLA.

Eventos de segurança e SLAs atribuídos.

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.	Até 1 hora útil	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	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 8 horas úteis (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 8 horas úteis (1 dia útil)	Até 40 horas úteis (5 dias úteis)
Projetos / Demandas Planejadas	Implementação de novas soluções de infraestrutura. Consultoria para elaboração de projetos arquiteturais 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

Para que o SLA de Gravidade Crítica (1h resposta / 2h resolução) seja viável e considerando que o firewall estará operando inline (todo o tráfego passa por ele), a CONTRATADA deve garantir a presença física, sem quarteirização, sempre que:

a) Houver falha de hardware que impeça o funcionamento do software de segurança;
b) Ocorrer o isolamento de rede que impossibilite o acesso remoto da equipe de SOC (Security Operations Center);
c) For necessária a troca de mídias físicas.

Portanto, a CONTRATADA deve manter equipe local, ou que esteja em local que possa atender o critério de "Impossibilidade de Acesso Remoto por Falha de Link ou Hardware" dentro duas horas para atendimento de situações críticas ou de alto impacto.

8. Declaração da Viabilidade da Contratação

Com base no estudo apresentado, declaramos viável a contratação de uma solução SECaaS para firewall, antivírus e monitoramento. A solução oferece a melhor relação custo-benefício e atende plenamente às necessidades identificadas.

Lajeado, 11/03/2026

Responsável pela Elaboração
Luis Antônio Schneiders

Secretário Responsável
Patrícia Haentssgen