PREFEITURA MUNICIPAL DE SANTA MARIA/RS

Estudo Técnico Preliminar 117/2026

1. Informações Básicas

Número do processo: 55/2026

2. Descrição da necessidade

Considerando que as soluções corporativas de segurança digital são indispensáveis para mitigar riscos operacionais, proteger dados sensíveis sob a guarda da administração pública e reduzir a vulnerabilidade a ataques de ransomware e outros malwares, o Município de Santa Maria adota, historicamente, políticas proativas de proteção de sua infraestrutura tecnológica.

Desde 2015, por meio dos Contratos nº 45/2015 e nº 23/2020, o município manteve soluções baseadas no modelo EPP (Endpoint Protection Platform). Embora adequadas ao cenário tecnológico da época, tais ferramentas atuavam de forma puramente reativa, limitando-se ao bloqueio de ameaças previamente identificadas por assinaturas. Esse modelo mostrava-se vulnerável a ataques de "dia zero" (zero-day), nos quais ameaças inéditas podiam transpor as defesas sem detecção, expondo a arquitetura de rede municipal a riscos severos de integridade e descontinuidade dos serviços públicos essenciais prestados aos cidadãos.

Com a evolução do cenário de ameaças, o mercado tecnológico migrou para o modelo EDR (Endpoint Detection and Response), o qual passou a utilizar Inteligência Artificial e análise de heurística comportamental para identificar anomalias em tempo real, independentemente do histórico prévio do artefato malicioso. Contudo, a visibilidade desse modelo restringe-se estritamente aos endpoints (computadores e servidores locais).

Mais recentemente, o mercado consolidou o salto tecnológico para as soluções XDR (Extended Detection and Response). Esse modelo estende a capacidade analítica e de inteligência para além das máquinas físicas, correlacionando o comportamento da rede de dados, e-mails e ambientes em nuvem de forma integrada, o que permite o bloqueio automatizado e centralizado de investidas complexas.

Essa evolução mostrou-se estritamente necessária diante de dados consolidados por relatórios globais de ameaças cibernéticas (como os indicadores publicados pela empresa de segurança CrowdStrike), que apontam que o tempo médio de eclosão e propagação de um ataque digital contemporâneo atinge a criticidade em cerca de 27 segundos. Diante de tal velocidade, a intervenção puramente humana torna-se ineficaz sem o apoio de automação integrada.

Em consonância com a evolução tecnológica e com a necessidade de manutenção da segurança da infraestrutura municipal, o Município possui histórico de utilização de soluções corporativas de proteção digital, incluindo as licenças da fabricante Kaspersky adquiridas por meio do Contrato nº 23/2020 e a solução XDR implantada posteriormente por meio do Contrato nº 831/2023.

Considerando o encerramento da vigência do Contrato nº 831/2023 em dezembro de 2026, torna-se necessária a realização de nova contratação para assegurar a continuidade da proteção dos equipamentos, servidores e dados institucionais, bem como promover a atualização tecnológica das ferramentas de segurança utilizadas pela Administração.

3. Área requisitante

Área Requisitante	Responsável
Luciano da Silveira Roepke	Superintendência de Tecnologia da Informação

4. Necessidades de Negócio

Renovação e evolução tecnológica das licenças de antivírus corporativo originalmente adquiridas sob o Contrato nº 23/2020. A migração do modelo legado EPP para a arquitetura proativa e integrada do tipo XDR é indispensável para neutralizar ameaças avançadas e ataques de "dia zero" (zero-day). Adicionalmente, faz-se necessária a implementação de uma camada de segurança gerenciada (MXDR - Managed Extended Detection and Response)

para os servidores de rede críticos expostos à internet, combinando a tecnologia de detecção automatizada com o monitoramento proativo, triagem e resposta a incidentes 24/7 realizada por um Centro de Operações de Segurança (SOC) especializado do fornecedor.

A contratação deverá atender à necessidade de proteção centralizada do parque tecnológico municipal, contemplando estações de trabalho e ambientes virtualizados, mediante recursos de detecção, análise e resposta a ameaças cibernéticas.

Para as estações de trabalho, busca-se assegurar a proteção contínua dos equipamentos utilizados pelos servidores municipais, com gerenciamento centralizado e mecanismos avançados de detecção e resposta a incidentes.

Para os ambientes virtualizados que hospedam serviços e sistemas institucionais críticos, além da proteção tecnológica, faz-se necessária a disponibilização de serviço gerenciado MXDR, com monitoramento especializado em regime 24x7, permitindo a identificação, análise, comunicação e resposta a incidentes de segurança.

A contratação também deverá contemplar os serviços de instalação, configuração e transferência de conhecimento, garantindo a adequada implantação da solução e a capacitação da equipe técnica responsável por sua administração.

5. Necessidades Tecnológicas

Além de renovar as licenças será necessária a instalação, configuração e treinamento da solução no parque de máquinas do município, pois houve mudanças na equipe e se torna necessário expandir o conhecimento para todos os envolvidos.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Para a definição da solução de TIC, foram considerados o histórico de utilização de ferramentas de segurança digital pelo Município, a infraestrutura tecnológica existente, a necessidade de gerenciamento centralizado, a compatibilidade com os ambientes computacionais utilizados e os custos envolvidos na implantação e manutenção da solução.

Também foram considerados os requisitos de atualização tecnológica, capacidade de detecção e resposta a ameaças, monitoramento especializado dos ambientes críticos, suporte técnico e continuidade operacional.

A solução deverá atender às necessidades de proteção das estações de trabalho e dos ambientes virtualizados, contemplando os recursos de XDR e MXDR, bem como os serviços necessários à sua implantação e operação.

7. Estimativa da demanda - quantidade de bens e serviços

Item	Descrição	Unidade de Medida	Quantidade
1	Renovação de Licença de Antivírus Kaspersky para Estação de Trabalho	Unidade	2.000
2	Renovação de Licença de Antivírus Kaspersky para Ambiente Virtualizado	Unidade	200
3	Serviço de Instalação e Configuração da Solução Antivírus, com Treinamento "Hands-On" da Solução de Antivírus	Serviço	1

8. Levantamento de soluções

Solução 1: Contratação de novo licenciamento SAAS

Solução 2: Renovação e atualização de licenças já adquridas

9. Análise comparativa de soluções

Solução 1: Contratação de novo licenciamento SAAS

O atual contrato nº 831/2023, entrega licenças do tipo XDR porém possui um alto custo unitário por licença, em um parque de máquinas com alto número de endpoints o custo anual se torna um empecilho no atual cenário econômico do Município.

Solução 2: Renovação e atualização de licenças já adquridas

A contratação de solução de outro fabricante poderá atender aos requisitos de segurança estabelecidos, entretanto deverá ser considerada a necessidade de implantação de uma nova plataforma, migração dos ambientes existentes, adaptação das políticas de segurança, capacitação da equipe técnica e eventuais custos de transição.

A manutenção e atualização das licenças Kaspersky anteriormente adquiridas apresenta potencial vantagem operacional, considerando o conhecimento já existente na equipe técnica e a possibilidade de aproveitamento da estrutura tecnológica previamente utilizada, condicionada à confirmação das condições técnicas e comerciais de atualização dessas licenças.

A alternativa de atualização e ampliação da solução Kaspersky permite contemplar tanto as estações de trabalho quanto os ambientes virtualizados, incluindo o serviço gerenciado MXDR para os servidores críticos, além dos serviços de implantação e capacitação técnica.

A definição da solução deverá considerar a compatibilidade tecnológica, os custos totais de implantação e operação, as funcionalidades disponibilizadas e a capacidade de atendimento aos requisitos de segurança da infraestrutura municipal.

10. Registro de soluções consideradas inviáveis

Considerando a importância da solução de antivírus para garantir segurança e confiabilidade da informações mantidas pelo Município de forma digital, considera-se inviável a não contratação de solução de antivírus, pois desta forma o datacenter estaria vulnerável a ataques cibernéticos.

11. Análise comparativa de custos (TCO)

Solução	Valor Unitário da Licença para 36 meses	Fonte
Contratação de novo licenciamento SAAS	R$ 632,96	Contrato 831/2026
Renovação e atualização de licenças já adquridas	R$ 466,56	Preço de Referência - R$ 12,96 x 36 meses

Para fins de comparação, foi considerado o valor unitário da solução XDR contratada por meio do Contrato nº 831/2023, correspondente a R$ 632,96 por licença para o período de 36 meses, em comparação com o valor mensal de referência de R$ 12,96 por licença da solução Kaspersky, multiplicado pelo mesmo período, resultando em R$ 466,56 por licença.

A comparação indica uma diferença nominal de aproximadamente 26,29% no custo unitário de licenciamento. Ressalta-se que os valores possuem caráter referencial, uma vez que os escopos das soluções não são integralmente equivalentes, devendo ser consideradas, na avaliação da vantajosidade, as funcionalidades disponibilizadas, os serviços associados, os custos de implantação e as condições de suporte e monitoramento.

12. Descrição da solução de TIC a ser contratada

A solução de TIC a ser contratada compreende:

- **Proteção das estações de trabalho:** disponibilização de 2.000 licenças da solução Kaspersky XDR, contemplando recursos de proteção, detecção e resposta a ameaças, com gerenciamento centralizado.
- **Proteção dos ambientes virtualizados:** disponibilização de 200 licenças da solução Kaspersky MXDR, contemplando recursos de proteção e serviço gerenciado de monitoramento especializado em regime 24x7, incluindo identificação, análise, comunicação e resposta a incidentes de segurança.
- A solução deverá permitir o gerenciamento centralizado dos ambientes protegidos e assegurar a integração dos recursos de detecção e resposta a ameaças, conforme as especificações técnicas estabelecidas no Termo de Referência.

- **Implantação e configuração:** prestação de serviços técnicos para instalação, configuração da plataforma, adequação das políticas de segurança e disponibilização da solução nos ambientes tecnológicos do Município.

- **Transferência de conhecimento:** realização de treinamento técnico prático (hands-on) para a equipe da Superintendência de Tecnologia da Informação, visando capacitar os servidores responsáveis pela administração e operação da solução.

13. Estimativa de custo total da contratação

Valor (R$): 2.164.800,00

O custo mensal estimado é R$ 35.200,00, totalizando R$ 2.164.800,00 para 60 meses.

14. Justificativa técnica da escolha da solução

A escolha de renovação das licenças de Kaspersky XDR em detrimento das tecnologias legadas do mercado como EPP e EDR fundamenta-se nos seguintes critérios técnicos:

- As soluções do tipo EPP demonstraram-se obsoletas frente ao atual panorama do cibercrime. Por dependerem da identificação prévia de assinaturas de malware, tais ferramentas mostram-se totalmente ineficazes contra ataques de "dia zero" (zero-day) e ameaças que utilizam executáveis legítimos do sistema operacional para fins maliciosos (Living off the Land). A adoção de uma solução puramente preventiva baseada em EPP representaria um retrocesso crítico na segurança digital do Município, expondo os dados dos cidadãos e os sistemas de arrecadação e gestão a riscos severos de interrupção.

- Embora as ferramentas de EDR agreguem Inteligência Artificial para análise comportamental nas estações de trabalho e servidores, sua capacidade de detecção é limitada e isolada. O ecossistema tecnológico do Município de Santa Maria é composto por uma infraestrutura híbrida complexa, que envolve tráfego de rede local, serviços em nuvem, sistemas de e-mail institucional e gerenciamento de identidades.

- A tecnologia XDR justifica-se tecnicamente por sua capacidade de transceder o endpoint, coletando, correlacionando e analisando telemetrias de múltiplas camadas da infraestrutura (Rede, E-mail, Nuvem e Endpoint) de forma unificada. Isso mitiga o problema dos "pontos cegos" de segurança, nos quais um ataque avança pela rede silenciosamente sem que o agente do computador local perceba a movimentação lateral.

- Conforme dados consolidados do Relatório Global de Ameaças da CrowdStrike, o tempo médio para que um atacante consiga romper o perímetro e iniciar a movimentação lateral ou criptografia de dados reduziu-se para a criticidade de 27 segundos. Diante dessa velocidade, qualquer processo de resposta que dependa exclusivamente de análise e intervenção humana manual torna-se inócuo. A solução XDR justifica-se pela sua capacidade de automação correlacionada, permitindo que, ao detectar uma atividade suspeita no fluxo de e-mails ou na rede, o sistema isole automaticamente o endpoint afetado e bloqueie a ameaça de forma global na velocidade exigida pelo cenário de risco atual.

Justificativa da escolha da fabricante Kaspersky

A indicação da solução Kaspersky considera o histórico de utilização de ferramentas dessa fabricante pelo Município, especialmente as licenças adquiridas por meio do Contrato nº 23/2020, bem como o conhecimento técnico acumulado pela equipe responsável pela administração da infraestrutura de segurança da informação.

A continuidade da utilização da plataforma poderá proporcionar aproveitamento do conhecimento operacional existente, redução dos esforços de adaptação da equipe técnica e menor necessidade de reestruturação dos procedimentos e políticas de segurança já estabelecidos.

A eventual substituição da plataforma demandaria avaliação dos impactos decorrentes da migração tecnológica, incluindo implantação de nova ferramenta, adaptação das políticas de segurança, capacitação dos profissionais envolvidos e compatibilidade com os ambientes computacionais existentes.

Dessa forma, a manutenção da padronização tecnológica constitui alternativa a ser considerada sob os aspectos de continuidade operacional, compatibilidade, gestão e economicidade, desde que demonstradas documentalmente as condições de atualização das licenças preexistentes e a efetiva vantagem técnica e econômica da solução escolhida.

A contratação não pressupõe exclusividade comercial da fabricante, devendo ser assegurada a participação de revendedores e fornecedores que atendam às condições técnicas e comerciais estabelecidas no procedimento licitatório.

15. Justificativa econômica da escolha da solução

A escolha da solução considera os aspectos de economicidade relacionados ao custo de licenciamento, implantação, operação e manutenção da infraestrutura de segurança digital do Município.

Na comparação referencial do custo unitário de licenciamento para o período de 36 meses, a solução Kaspersky apresentou valor estimado de R$ 466,56 por licença, considerando o preço mensal de R$ 12,96, em comparação com o valor unitário de R$ 632,96 registrado no Contrato nº 831/2023, representando diferença nominal de aproximadamente 26,29%.

Ressalta-se que essa comparação se limita ao custo unitário de licenciamento para estações de trabalho, não abrangendo integralmente os diferentes escopos e serviços associados às soluções.

A contratação pretendida possui valor global estimado de R$ 2.164.800,00, composto por R$ 2.112.000,00 referentes ao licenciamento das 2.000 estações de trabalho e 200 ambientes virtualizados pelo período de 60 meses, e R$ 52.800,00 referentes aos serviços de instalação, configuração e treinamento.

A análise de vantajosidade deverá considerar, além dos valores apresentados, as funcionalidades de proteção XDR e monitoramento MXDR, os níveis de serviço, os custos de implantação e a continuidade operacional da infraestrutura municipal.

A contratação plurianual também deverá ser avaliada quanto à sua vantagem econômica em relação a alternativas de menor duração, considerando os valores estimados, as condições comerciais e a continuidade dos serviços de proteção digital.

16. Benefícios a serem alcançados com a contratação

A contratação proporcionará ao Município de Santa Maria benefícios estratégicos, operacionais, econômicos e legais, destacando-se:

- Garantia de disponibilidade dos serviços públicos: redução dos riscos de indisponibilidade dos sistemas institucionais e dos serviços essenciais prestados à população, mediante mecanismos de prevenção, detecção e resposta a incidentes cibernéticos.
- Proteção do patrimônio digital: fortalecimento dos mecanismos de segurança dos equipamentos, servidores, sistemas e dados mantidos pelo Município.
- Resposta a incidentes em tempo adequado: disponibilização de recursos automatizados de detecção e resposta, associados ao monitoramento especializado dos ambientes críticos, permitindo maior agilidade na identificação e tratamento de ameaças.
- Visibilidade da infraestrutura tecnológica: gerenciamento centralizado dos ambientes protegidos, possibilitando maior acompanhamento dos eventos de segurança e identificação de comportamentos suspeitos.
- Otimização das atividades da equipe técnica: redução da necessidade de intervenções exclusivamente manuais e disponibilização de ferramentas que auxiliem os profissionais da STI na administração e monitoramento da segurança digital.
- Economicidade e racionalização dos recursos públicos: busca pela melhor relação entre custo e benefício, considerando o aproveitamento da experiência técnica existente, os custos de implantação, a atualização tecnológica e os valores de licenciamento e serviços associados.
- Prevenção de prejuízos financeiros e operacionais: mitigação dos riscos de interrupção dos serviços públicos, perda de informações e necessidade de contratações emergenciais decorrentes de incidentes de segurança.
- Conformidade com a LGPD: fortalecimento dos mecanismos de proteção dos dados pessoais tratados e armazenados pelo Município, contribuindo para a segurança e a continuidade dos serviços institucionais.

17. Providências a serem Adotadas

- Configuração e disponibilização de servidor de rede virtualizado para instalação e configuração da solução.

- Disponibilização de acesso via VPN para os técnicos da Contratada realizarem as configurações necessárias.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

Esta equipe de planejamento declara **viável** esta contratação com base neste Estudo Técnico Preliminar.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

SABRINA MEDIANEIRA DA SILVA AVILA

Equipe de apoio

Assinou eletronicamente em 04/11/2026 às 10:32:07.