ESTUDO TÉCNICO PRELIMINAR

1. INFORMAÇÕES BÁSICAS:

Secretaria Requisitante: Secretaria Municipal de Administração

Processo SEI n° 25.0.000071226-7

2 . DESIGNAÇÃO DA EQUIPE DE PLANEJAMENTO:

Nome: Guilherme Dionier Gasparetto

Matrícula: 161

Nome: Leandro Wille Della Pace da Silva

Matrícula: 127

Nome: Marcelo Weiblen dos Santos

Matrícula: 62

Nome: João Francisco Lopes dos Santos

Matrícula: 157

3. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO:

3.1. Conforme dispõe a Lei nº 14.133/2021, a contratação de bens e serviços pela Administração Pública deve estar fundamentada na demonstração da necessidade, no atendimento ao interesse público e na observância dos princípios da legalidade, impessoalidade, moralidade, publicidade, eficiência, economicidade e motivação dos atos administrativos;

3.2. De acordo com o Relatório de Riscos Globais 2022 do Fórum Econômico Mundial, a crescente dependência de sistemas digitais vem transformando profundamente a sociedade, elevando a exposição a ameaças cibernéticas em nível superior à atual capacidade de prevenção e resposta. Ataques direcionados a infraestruturas críticas, disseminação de desinformação e fraudes têm impactado diretamente a confiança da população nessas plataformas.

Nesse contexto, a evolução constante do crime cibernético impõe às organizações públicas a necessidade de atualização permanente de suas estratégias e arquiteturas de segurança da informação, de modo a garantir a continuidade da prestação dos serviços públicos, a preservação do exercício da cidadania e a proteção das liberdades individuais, mesmo diante de cenários adversos.

Acrescenta-se que a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) estabelece, em seu art. 46, que agentes de tratamento de dados

pessoais devem adotar medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

A Prefeitura Municipal de Canoas (PMC), em seu atual parque tecnológico, administra aproximadamente 4.000 estações de trabalho, 300 servidores virtuais, 5466 usuários ativos de rede, além de storages e outros ativos críticos que processam e armazenam informações institucionais. Tais ativos necessitam de proteção contínua e robusta contra incidentes de segurança, visando garantir a integridade, confidencialidade e disponibilidade das informações.

Para atender a essa demanda, a Prefeitura Municipal de Canoas faz uso, desde 2014, aproximadamente, de soluções corporativas de segurança da informação desenvolvidas pela empresa Trend Micro, incluindo:

a. Trend Micro Enterprise Security for Endpoint Suite Advanced (Apex One) – voltada à proteção de estações de trabalho (endpoints);
b. Trend Micro Deep Security Compliance Pack - voltada à proteção servidores computacionais;
c. Trend Micro Deep Discovery Inspector Model VA 250 - voltado à análise de perímetros de redes.

A solução é estruturada em módulos que atuam de forma integrada, cobrindo diferentes camadas de defesa e ampliando a superfície de proteção do ambiente computacional da Prefeitura.

O histórico de adoção e expansão da solução Trend Micro na Prefeitura de Canoas evidência a consolidação das ferramentas utilizadas como parte essencial da política de segurança cibernética desta administração pública.

Considerando o cenário atual de elevação dos riscos cibernéticos, a relevância dos serviços prestados pela Prefeitura Municipal de Canoas à sociedade e as obrigações legais de proteção de dados e continuidade de serviços essenciais, a presente contratação visa assegurar a manutenção e evolução da infraestrutura de segurança da informação, garantindo níveis adequados de proteção e conformidade com as normas vigentes;

3.3. O presente Estudo Técnico Preliminar tem por objetivo avaliar, justificar e subsidiar a contratação de solução integrada de segurança da informação, contemplando licenciamento, aquisição de solução, atualização e suporte técnico especializado, com vistas à proteção das estações de trabalho, servidores, inspeção e análise de segurança em perímetros de redes e proteção para os sistemas de missão críticos da Prefeitura Municipal de Canoas, com integração aos sistemas de monitoramento existente e/ou que vierem a ser adquiridos, visando garantir a alta disponibilidade do ambiente de TI (tecnologia da Informação), pelo período inicial de 12 (doze) meses com a possibilidade de renovação pelo período estabelecido em Lei;

3.4. A finalidade ainda consiste em mitigar eventuais riscos quando se faz a análise dos fatores que contribuíram e/ou ainda contribuem para a problematização da situação a ser resolvida, as possíveis soluções e alternativas para a consecução das atividades de responsabilidade da Administração.

3.5. Esse Estudo Técnico Preliminar tem por base a Lei 14.133/2021, respeitando-se também as normativas vigentes no município e as recomendações emanadas pelos Órgãos de Controle.

4. DESCRIÇÃO DOS REQUISITOS PARA A CONTRATAÇÃO:

4.1. As obrigações firmadas entre a CONTRATANTE e a CONTRATADA serão formalizadas por meio de respectivo Contrato, observando-se as condições estabelecidas nos Termos de Referência, Edital, seus anexos e na legislação vigente.

4.2. OBJETO

4.2.1. Contratação de solução integrada de segurança da informação, contemplando licenciamento, aquisição de solução, atualização e suporte técnico especializado, com vistas à proteção das estações de trabalho, servidores, inspeção e análise de segurança em perímetros de redes para os sistemas de missão críticos da Prefeitura Municipal de Canoas;

4.2.2. Às soluções deverão contemplar recursos de prevenção, detecção e resposta a ameaças, tais como antivírus corporativo, firewall de host, prevenção contra intrusões (Host Intrusion Prevention System – HIPS), proteção contra malware, virtual patching, reputação web (Web Reputation) e proteção de rede, com gerenciamento centralizado e integração entre módulos, de forma a garantir a integridade, confidencialidade e disponibilidade das informações institucionais;

4.2.3. Na presente contratação, todas as ferramentas da fabricante Trend Micro atualmente em produção serão unificadas em um mesmo contrato com o objetivo de consolidar administrativamente o ambiente de segurança do PMC, organizando e simplificando os processos de renovação futuros.

4.2.4. As soluções de segurança corporativa presentes no escopo desta contratação são:

4.2.4.1. Antivírus - proteção de estação de trabalho: Diferentemente de um antivírus para uso pessoal, este tipo de solução corporativa busca inibir a incidência de vírus em ambientes amplos e complexos. Dispõe de arquitetura e ferramentas administrativas que permitem sua atuação e manutenção nestes ambientes de forma gerenciável em uma única interface;

4.2.4.2. Proteção contra malwares e pragas virtuais: Atua no monitoramento, detecção e resposta às ameaças de segurança cibernética. A solução utiliza de padrões conhecidos e desconhecidos e análise de reputação para detectar tentativas e ataques cibernéticos a infraestrutura da PMC;

4.2.4.3. Proteção do ambiente de virtualização: Solução em nuvem para detecção e resposta contra vulnerabilidades, malwares e mudanças não autorizadas em ambientes físicos, virtuais, nuvem e contêineres;

4.2.4.4. Proteção de perímetro de rede: É uma solução de segurança de rede desenvolvida para detectar, analisar e responder a ameaças avançadas, ataques direcionados (targeted attacks) e malware de difícil detecção, incluindo ameaças persistentes avançadas (Advanced Persistent Threats – APTs). Opera por meio da inspeção profunda do tráfego de rede (network traffic analysis), identificando comunicações suspeitas, comportamentos anômalos e padrões associados a ataques direcionados, mesmo quando utilizam técnicas de evasão como criptografia, portas não padrão e protocolos legítimos.

4.2.5. É importante ressaltar a importância da integração entre essas ferramentas, garantindo gerência global sobre as mesmas e a capacidade de correlacionar eventos detectados nas diferentes soluções. A contratação destas ferramentas justifica-se para garantir a segurança do ambiente de TIC da Prefeitura Municipal de Canoas.

4.3. OBJETIVOS

A contratação da solução de segurança tem por objetivos:

4.3.1. Manter os softwares das soluções ora implantadas, visando proteção de rede, detecção e prevenção contra ameaças;

4.3.2. Minimizar os riscos de interrupção da proteção de cibersegurança;

4.3.3. Proteger os ambientes on premises e em nuvem, de maneira integrada;

4.3.4. Ampliar as camadas de proteção contra riscos cibernéticos com ferramentas avançadas.

4.4. BENEFÍCIOS

Os benefícios esperados com esta contratação são:

4.4.1. Garantir a alta disponibilidade e integridade do ambiente tecnológico da Prefeitura Municipal de Canoas;

4.4.2. Aumentar a segurança da rede, com agentes instalados em cada computador, minimizando os problemas relacionados às estações de trabalho, cite-se: Disseminação de pragas virtuais (vírus, trojans, malware e códigos maliciosos);

4.4.3. Promover melhorias no processo de monitoramento, através da predefinição e personalização de gráficos de monitoramento e envio de notificações;

4.4.4. Garantir o aproveitamento do conhecimento histórico acerca das ferramentas;

4.4.5. Garantir suporte técnico avançado;

4.4.6. Promover a evolução das ferramentas para modelo SaaS em nuvem.

5. LEVANTAMENTO DE MERCADO:

5.1. Em atendimento ao inciso III do art. 9º da IN nº 58/2022, foi realizado levantamento de mercado com o objetivo de identificar soluções de segurança da informação equivalentes ou superiores à atualmente em uso, observando aspectos técnicos, operacionais e econômicos.

Foram consultadas propostas junto a fornecedores especializados, além da análise de contratações similares em outros entes públicos, para verificação de metodologias, tecnologias e inovações aplicáveis. A pesquisa considerou soluções líderes de mercado em proteção de endpoints, servidores, análise de tráfego e correlação de eventos de segurança, observando compatibilidade com a infraestrutura tecnológica existente na Prefeitura Municipal de Canoas e integração com as ferramentas de monitoramento já implantadas.

As cotações e dados coletados evidenciaram que a solução da fabricante Trend Micro mantém aderência plena aos requisitos técnicos e operacionais, com histórico consolidado de uso no órgão, garantindo continuidade operacional, evitando custos adicionais com substituição ou migração e minimizando riscos de indisponibilidade de serviços críticos;

5.2. Em atendimento ao princípio da seleção da proposta mais vantajosa para a Administração Pública, conforme disposto nos arts. 11, inciso I, e 40, inciso I, da Lei no 14.133/2021, e buscando assegurar a ampla competitividade, a economicidade e a eficiência na contratação, os posteriores documentos, termo de referência e edital serão estruturados em itens distintos para cada tipo de aquisição/atualização/licenciamento/suporte e em lote único;

5.3. Considerando que todos os softwares pertinentes a este processo são oriundos de um mesmo fabricante e que os fornecedores costumam obter descontos mais significativos à medida que efetuam compras em maior escala, optamos por manter os objetos dessa aquisição em lote único, visando angariar o melhor preço para a Administração. Ressalta-se que tal decisão não acarreta quaisquer prejuízos à ampla concorrência de licitantes interessados em fornecer os objetos dispostos nesta contratação;

5.4. A metodologia utilizada para determinar este valor é fundamentada na mediana de preços, que representa um indicador estatístico confiável para a avaliação de custos. Dúvidas sobre a metodologia aplicada podem ser consultadas no seguinte link: https://www.gov.br/ancine/pt-br/acesso-a-informacao/perguntas-frequentes1/

licitacoes-e-contratacoes-diretas/quando-devo-utilizar-media-mediana-ou-menor-preco;

5.5. É importante ressaltar que o valor estimado pode ser ajustado com base nas propostas recebidas durante o processo de aferição pública, pois os valores foram aferidos utilizando o painel de preços do Governo Federal (https://paineldeprecos.planejamento.gov.br/analise-materiais) e também no painel LicitaCon Cidadão. A transparência e a busca pela melhor relação custo-benefício devem ser prioridades durante todo o processo;

5.6. Em razão da alta especificidade técnica dos itens, não foi possível obter orçamentos prévios para exatamente todos os itens a serem adquiridos. Sendo assim, para assegurar a continuidade do processo de contratação e evitar prejuízo ao interesse público, a composição estimativa de preços será baseada em pesquisas de mercado disponíveis, valores referenciais de contratos similares firmados por outros entes públicos e consultas técnicas, em conformidade com o disposto no art. 23, inciso III, da Lei no 14.133/2021;

5.7. LEVANTAMENTO DE PREÇOS DE MERCADO

Item	Objeto do item	Pregão Eletrônico 132/2025 Prefeitura Municipal de Caxias do Sul	Pregão Eletrônico - 131/2024 Prefeitura Municipal de Farroupilha	Pregão Eletrônico - 174/2024 Prefeitura Municipal de Panambi	Pregão Eletrônico 131/2025 Pref. de Americana	Pregão Eletrônico 12/2025 Secret, de Adm. Estado do Piauí	Proposta comercial Bence	Proposta comercial Grupo NTSEC
1	Trend Micro - Endpoint Security CORE - VORA0029		R$ 70,40	R$ 151,76	R$ 79,35		R$ 75,82	R$ 119,02
2	Trend Micro - Endpoint Security PRO - VORA0042	R$ 1.990,00		R$ 1.896,99	R$ 769,19	R$ 1.237,62	R$ 1.020,12	R$ 2.622,53
3	Trend Micro - Deep Discovery Inspector Series Virtual 500 - DDNA0036					R$ 155.874,87	R$ 174.123,25	R$ 234.658,51
4	Horas técnica de suporte e/ou consultoria	R$ 370,00					R$ 400,00	R$ 507,00

5.8. ANÁLISE DAS ALTERNATIVAS POSSÍVEIS

5.8.1. Em conformidade com o disposto no art. 9º, inciso III, da Instrução Normativa nº 58/2022 e com os princípios da Lei nº 14.133/2021, foram avaliados três cenários técnicos e administrativos para atendimento da

necessidade de proteção integrada das estações de trabalho, servidores e perímetros de rede da Prefeitura Municipal de Canoas.

5.8.2. Solução 1 – Manutenção da plataforma Trend Micro

5.8.2.1. Descrição técnica:

5.8.2.1.1. Manter a contratação das soluções de segurança da informação já implantadas, desenvolvidas pela Trend Micro (Apex One, Deep Security, Deep Discovery Inspector), com atualização de licenças, suporte técnico especializado e integração contínua com a infraestrutura existente;

5.8.2.1.2. O modelo atual cobre cerca de 4.000 endpoints, 150 servidores e ativos críticos, com gestão centralizada e recursos como antivírus corporativo, firewall de host, virtual patching, HIPS, proteção web, antispam e sandboxing;

5.8.2.2. Justificativa administrativa:

5.8.2.2.1. Uso disseminado e consolidado no ambiente da Prefeitura desde 2014, com equipe técnica treinada e processos operacionais ajustados;

5.8.2.2.2. Continuidade operacional sem necessidade de adaptação, minimizando riscos de indisponibilidade;

5.8.2.2.3. Preservação de investimentos já realizados em licenciamentos e treinamentos;

5.8.2.2.4. Menor risco de incompatibilidade com sistemas existentes, garantindo economicidade e eficiência (art. 5º, Lei 14.133/2021).

5.8.2.3. Vantagens:

5.8.2.3.1. Reduz curva de aprendizado e custos indiretos;

5.8.2.3.2. Evita aquisições complementares para compatibilidade;

5.8.2.3.3. Tempo de implantação praticamente imediato.

5.8.3. Solução 2 – Substituição por solução equivalente de outro fabricante

5.8.3.1. Descrição técnica:

5.8.3.1.1. Trocar a solução atual por produto de segurança da informação de fabricante concorrente (ex.: Palo Alto, Trellix, SentinelOne), com funcionalidades equivalentes de proteção de endpoints, servidores e rede.

5.8.3.2. Justificativa administrativa:

5.8.3.2.1. Possibilidade de avaliação de novas funcionalidades ou modelos comerciais;

5.8.3.2.2. Potencial acesso a tecnologias emergentes ou formatos de licenciamento alternativos;

5.8.3.3. Desvantagens:

5.8.3.3.1. Necessidade de nova implantação, migração e reconfiguração de políticas de segurança;

5.8.3.3.2. Treinamento adicional da equipe técnica e de suporte;

5.8.3.3.3. Risco elevado de incompatibilidade ou perda temporária de cobertura durante a transição;

5.8.3.3.4. Custo potencialmente maior na etapa inicial (capex + opex).

5.8.4. Solução 3 – Arquitetura híbrida com múltiplos fornecedores

5.8.4.1. Descrição técnica:

5.8.4.1.1. Implantar solução de segurança distribuída, combinando ferramentas de diferentes fabricantes para atender a camadas específicas — por exemplo, um fornecedor para endpoints, outro para servidores e outro para análise perimetral.

5.8.4.2. Justificativa administrativa:

5.8.4.2.1. Possibilidade de especialização por camada de proteção;

5.8.4.2.2. Redução de dependência de um único fornecedor.

5.8.4.3. Desvantagens:

5.8.4.3.1. Aumento da complexidade de gestão, exigindo múltiplos consoles e integrações;

5.8.4.3.2. Maior custo de operação devido à fragmentação contratual e de suporte;

5.8.4.3.3. Dificuldade na correlação de eventos e unificação de políticas de segurança;

5.8.4.3.4. Maior esforço administrativo para renovações e fiscalizações contratuais.

5.8.5. Quadro Comparativo – Análise Custo x Risco

Soluções	Descrição	Custo Estimado	Risco Operacional	Observações
1 – Manutenção da plataforma Trend Micro	Renovação das licenças, atualização e suporte das soluções Trend	**Baixo** – Custos restritos à renovação contratual, sem necessidade de	**Baixo** – Continuidade imediata, equipe treinada, integração já	Maximiza investimentos já realizados; preserva compatibilidade

	Micro já implantadas (Apex One, Deep Security, Deep Discovery Inspector).	migração ou aquisição de novos equipamentos.	validada, mínimo risco de indisponibilidade.	e desempenho; reduz curva de aprendizado.
2 - Substituição por solução equivalente de outro fabricante	Troca da plataforma atual por produto concorrente com funcionalidades similares.	**Alto** – Inclui custos de licenciamento, implantação, migração, treinamento e possíveis ajustes de infraestrutura.	**Médio/Alto** – Risco de incompatibilidade, perda temporária de cobertura e aumento do tempo de resposta durante a transição.	Pode trazer novas funcionalidades, mas com risco elevado e alto custo inicial.
3 – Arquitetura híbrida com múltiplos fornecedores	Implantação de soluções distintas para cada camada (endpoint, servidor, perímetro).	**Médio/Alto** – Necessidade de múltiplos contratos, licenças, integrações e treinamentos específicos.	**Alto** – Complexidade operacional, dificuldades de correlação de eventos e gestão centralizada, risco de falhas por lacunas de integração.	Possibilidade de especialização por camada, mas aumenta o esforço administrativo e técnico.

5.8.6. A análise demonstra que a solução 1 apresenta o menor custo total de propriedade e o menor risco operacional, sendo tecnicamente e administrativamente a alternativa mais vantajosa. Além disso, mantém a conformidade com a Lei nº 14.133/2021, a LGPD e as melhores práticas de gestão de segurança da informação, preservando a eficiência e a economicidade na Administração Pública.

5.8.7. Portanto, a análise técnica e administrativa indica a Solução 1 – Manutenção da plataforma Trend Micro apresenta-se como a alternativa mais vantajosa para a Administração, por assegurar a continuidade da proteção, maximizar o aproveitamento dos investimentos já realizados, evitar riscos operacionais de migração e manter elevada a relação custo-benefício ao longo do ciclo de vida da contratação.

6. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO:

6.1. A solução objeto desta contratação consiste em um conjunto integrado de ferramentas corporativas de segurança da informação, voltadas à proteção de

estações de trabalho, servidores, perímetros de rede e serviços essenciais;

6.2. Inclui módulos para prevenção contra ameaças, detecção e resposta a incidentes, proteção contra malwares conhecidos e desconhecidos, firewall de host, Host Intrusion Prevention System (HIPS), virtual patching, reputação web (Web Reputation), antispam e sandboxing, todos gerenciados de forma centralizada;

6.3. O pacote contempla licenciamento, suporte técnico especializado, atualizações tecnológicas e manutenção preventiva/corretiva pelo período contratual, permitindo gestão unificada de incidentes e correlação de eventos de segurança, além de integração com sistemas de monitoramento existentes e futuros;

6.4. A escolha da solução Trend Micro se justifica pela elevada maturidade tecnológica, pela aderência à infraestrutura já implantada e pelo histórico de resultados satisfatórios, representando a alternativa mais vantajosa sob os aspectos de eficiência, economicidade e mitigação de riscos;

6.4.1. Fundamentação legal

6.4.1.1. A escolha da Solução 01 encontra respaldo nos princípios da eficiência, economicidade e continuidade do serviço público, conforme preconizado na Lei no 14.133/2021, especialmente:

- Art. 11, inciso I: Planejamento como princípio do processo licitatório;
- Art. 12, inciso VI: Avaliação das soluções que melhor atendam ao interesse público;
- Art. 115, inciso II: Justificativa técnica para escolha da solução mais vantajosa.

6.5. REQUISITOS GERAIS

6.5.1. Analisando as alternativas disponíveis e que atendam à necessidade da área requisitante, considerando a viabilidade técnica e econômica, a solução indicada pela Diretoria de Infraestrutura da Canoastec, é a realização de procedimento licitatório para aquisição de licenças das ferramentas de segurança do fabricante Trend Micro e suporte técnico especializado, de acordo com especificações comuns de mercado capazes de atender aos requisitos de negócio e ora já implementados na PMC;

6.5.2. As licenças devem suportar:

6.5.2.1. Licenças de solução de proteção para workstations (estações de trabalho) com sistema operacional Windows a partir da versão do Windows 10;

6.5.2.2. Licenças de solução de proteção para workstations (estações de trabalho) com sistema operacional Linux a partir da versões baseadas em Red Hat, Debian, Ubuntu e Suse;

6.5.2.3. Licenças de solução de proteção para workstations (estações de trabalho) com sistema operacional macOS a partir da versão Sonoma;

6.5.2.4. Licenças de solução de proteção para servers (servidores) com sistema operacional Windows a partir da versão do windows server 2008 R2;

6.5.2.5. Licenças de solução de proteção para servers (servidores) com sistema operacional Linux a partir da versões baseadas em Red Hat, Debian, Ubuntu e Suse;

6.5.2.6. Licenças da solução de análise de perímetros de redes:

6.5.2.6.1. VMware ESXi;

6.5.2.6.2. Hyper-V;

6.5.2.6.3. KVM.

6.5.3. As licenças devem ser emitidas para um prazo de 12 (doze) meses, tendo estas suporte e atualizações do fabricante por todo o período;

6.5.4. As soluções devem adotar um único console de segurança integrada que cubra estações de trabalho, servidores, ambientes de redes, gerenciamento de risco e superfície de ataques. Essa abordagem centralizada não apenas fortalece a postura de segurança, mas também simplifica a gestão e promove maior eficiência em toda a organização;

6.5.5. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

6.5.6. Deve permitir atualização incremental da lista de definições de vírus;

6.5.7. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

6.5.8. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

6.5.9. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

6.5.10. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

6.5.11. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pelo console de administração da solução completa;

6.5.12. Deve possibilitar instalação "silenciosa";

6.5.13. Deve possuir firewall integrado;

6.5.14. Deve possuir EDR - Detecção e Resposta a Ameaças;

6.5.15. Deve possuir XDR (em produto específico para esta funcionalidade) - Extended Detection and Response;

6.5.16. Deve possuir machine learning e behavioral analysis para detecção de ameaças;

6.5.17. Deve possuir console de gerenciamento centralizado de ambas as ferramentas de proteção de estações de trabalho e servidores;

6.5.18. Deve possuir whitelisting de aplicações pré-aprovadas para execução;

6.5.19. Deve permitir rollback de ações maliciosas;

6.5.20. Deve possuir capacidade de executar arquivos suspeitos em ambiente isolado (sandbox).

6.6. ITENS A SEREM ADQUIRIDOS

Item	Objeto do item	Descrição do item	Nº da licença
1	Trend Micro - Endpoint Security CORE	Licenças de solução de proteção para workstations (estações de trabalho)	VORA0029
2	Trend Micro - Endpoint Security PRO	Licenças de solução de proteção para servers (servidores)	VORA0042
3	Trend Micro - Deep Discovery Inspector Series Virtual 500	Licenças da solução de à análise de perímetros de redes	DDNA0036
4	Horas técnica de suporte e/ou consultoria	Horas técnicas de consultoria e/ou implementação das soluções com profissional certificado pelo fabricante	

6.6.1. ITEM 1 - DESCRIÇÃO DA SOLUÇÃO - Trend Micro - Endpoint Security CORE

6.6.1.1. Além dos requisitos já elencados nos Requisitos Gerais (tópico próprio) deve possuir, ainda, os requisitos listados abaixo;

6.6.1.2. Deverá possuir as seguintes opções de proteção:

6.6.1.2.1. Controle de aplicação;

6.6.1.2.2. DLP (data loss prevention);

6.6.1.2.3. Controle de dispositivos;

6.6.1.2.4. Firewall;

6.6.1.2.5. Machine Learning;

6.6.1.2.6. Escaneamento em tempo real;

6.6.1.2.7. Smart Scan;

6.6.1.2.8. Suspicious connection service;

6.6.1.2.9. Vulnerability protection;

6.6.1.2.10. Web reputation;

6.6.1.3. A solução deve atender a estações de trabalho com soluções de Sistemas Operacionais Windows, Linux e macOS;

6.6.1.4. Deve ser capaz de realizar a proteção a códigos maliciosos nos Sistemas Operacionais Windows, Linux e macOS;

6.6.1.5. Deve identificar e impedir infecções através de ameaças em arquivos, que executam diretamente em memória;

6.6.1.6. Deve identificar e impedir infecções através de ameaças em arquivos, que executem em dispositivos móveis;

6.6.1.7. Deve identificar e impedir infecções através de ameaças em arquivos, que sejam baixados diretamente da Internet;

6.6.1.8. Deve identificar e impedir infecções através de ameaças em links acessados diretamente da Internet;

6.6.1.9. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

6.6.1.9.1. Processos em execução em memória principal (RAM);

6.6.1.9.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

6.6.1.9.3. Arquivos compactados, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

6.6.1.9.4. Arquivos recebidos por meio de programas de comunicação instantânea tais como Whatsapp, Telegram, Facebook Messenger, Microsoft Teams, Zoom, Google Meet;

6.6.1.9.5. Arquivos recebidos a partir de sites Web;

6.6.1.9.6. Arquivos acessados ou recebidos por e-mail.

6.6.1.10. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

6.6.1.10.1. Em tempo real de arquivos acessados pelo usuário;

6.6.1.10.2. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

6.6.1.10.3. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

6.6.1.10.4. Por linha de comando parametrizável.

6.6.1.11. A funcionalidade de "Machine Learning" utilizando como fonte de aprendizado a rede de inteligência do fabricante, identificando os aspectos maliciosos, características de boa pontuação e correlacionando, no mínimo, com as seguintes técnicas de proteção a vetores de ataque:

6.6.1.11.1. Reputação de URL para exploração de navegadores, websites infectados e Office Exploits;

6.6.1.11.2. Reputação de arquivos para downloads de arquivos e anexos de e-mail.

6.6.1.12. Execução do instalador de software com classificação comportamental do instalador;

6.6.1.13. A console de gerenciamento deve permitir o gerenciamento das políticas de segurança através dos agentes instalados através da internet;

6.6.1.14. O módulo de controle de aplicações deve utilizar os conceitos de permissão explícita, informando as aplicações que podem executar; e de restrição explícita, informando aplicações que não podem executar;

6.6.1.15. Após as varreduras, a solução deve habilitar novas regras de proteção necessárias e desabilitar aquelas que já foram corrigidas com o patch oficial, de forma automática;

6.6.1.16. A solução deve ter capacidade de resposta aos incidentes, isolando os endpoints da rede, bloqueando ou coletando um arquivo para análise, bloqueando uma URL maliciosa, executando um comando remoto em PowerShell;

6.6.1.17. O administrador deve ter a possibilidade de definir quais componentes listados devem ser monitorados.

6.6.1.18. Deverá possuir proteção multicamadas;

6.6.1.19. Deverá combinar assinaturas tradicionais, análise comportamental e técnicas de machine learning para ampliar a detecção de ameaças conhecidas e desconhecidas;

6.6.1.20. Inclui proteção contra explorações de vulnerabilidades de dia zero e ataques direcionados;

6.6.1.21. Deverá possuir integração com Trend Vision One;

6.6.1.22. Permitir que alertas do Endpoint CORE sejam correlacionados em tempo real com dados de e-mail, rede e servidores;

6.6.1.23. Deverá gerar visibilidade unificada de incidentes, facilitando a resposta rápida a ataques multivetoriais;

6.6.1.24. Proteção contra Ransomware e Exploits de Memória;

6.6.1.25. Monitorar comportamentos suspeitos como criptografia em massa de arquivos;

6.6.1.26. Deverá detectar tentativas de execução maliciosa direto na memória, incluindo ataques fileless;

6.6.1.27. Deve possuir garantia e atualizações, correções e evoluções por toda a validade da licença;

6.6.1.28. Deve fornecer proteção em tempo real contra ataques de ransomware, spywares, trojans, vírus e worms;

6.6.1.29. Deverá possuir controle granular de políticas;

6.6.1.30. Deverá possibilitar a aplicação de diferentes políticas de segurança por grupo, departamento, tipo de dispositivo ou sistema operacional;

6.6.1.31. Políticas poderão ser ajustadas remotamente mesmo para máquinas fora da rede corporativa;

6.6.1.32. Deverá possuir atualizações automáticas e inteligentes;

6.6.1.33. Suporte a Smart Protection Network™, com atualizações em nuvem em tempo real;

6.6.1.34. Proteção de Navegação Segura (Web Security);

6.6.1.35. Avaliação em tempo real de URLs acessadas, com bloqueio de sites maliciosos, phishing e hospedagem de malware;

6.6.1.36. Deverá possuir a possibilidade de exportar logs em formatos padronizados (Syslog, CEF, JSON) para integração com SOCs, SIEM e plataformas de orquestração de resposta.

6.6.1.37. APIs abertas para automação e integração com ferramentas de gestão corporativa;

6.6.1.38. Possuir resposta rápida a incidentes (EDR Básico);

6.6.1.39. Deverá possuir alta disponibilidade e suporte;

6.6.1.40. Deverá possuir relatórios e auditoria de conformidade;

6.6.1.41. Dashboards em tempo real com visão de segurança por usuário e/ou dispositivo;

6.6.1.42. Relatórios exportáveis em formatos PDF/CSV para auditorias de conformidade (LGPD, ISO 27001, PCI-DSS, etc.).

6.6.2. ITEM 2 - DESCRIÇÃO DA SOLUÇÃO - Trend Micro - Endpoint Security PRO

6.6.2.1. Além dos requisitos já elencados nos Requisitos Gerais (tópico próprio) deve possuir as mesmas características do item 1 - Trend Micro - Endpoint Security CORE, além da demais especificadas abaixo;

6.6.2.2. Deverá possuir as seguintes opções de proteção:

6.6.2.2.1. Anti-Malware;

6.6.2.2.2. Web Reputation;

6.6.2.2.3. Firewall;

6.6.2.2.4. Intrusion Prevention;

6.6.2.2.5. Integrity Monitoring;

6.6.2.2.6. Log Inspection;

6.6.2.2.7. Application Control;

6.6.2.2.8. Activity Monitoring;

6.6.2.2.9. Device Control.

6.6.2.3. O console de gerenciamento deve permitindo o gerenciamento das políticas de segurança através da Internet;

6.6.2.4. Deve possuir integração com a solução de Detecção e Resposta Avançada de Ataques (XDR);

6.6.2.5. O Console deve ser gerenciada por console Web, compatível com pelo menos os browsers Microsoft Edge, Firefox e Google Chrome;

6.6.2.6. O console de administração deve permitir o envio de notificações via SMTP;

6.6.2.7. Todos os eventos e ações realizadas no console de gerenciamento precisam ser gravados, visando a auditoria;

6.6.2.8. Deve permitir a criação de widgets para facilitar a administração e visualização dos eventos;

6.6.2.9. A funcionalidade de anti-malware deve possuir as seguintes características:

6.6.2.9.1. Deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e agendamento, com possibilidade de tomada de ações distintas para cada tipo de ameaça;

6.6.2.9.2. Deve possibilitar a criação de listas de exclusão, para que o processo de inspeção não execute a varredura em determinados diretórios ou arquivos do sistema operacional;

6.6.2.9.3. Deve possuir listas de exclusão separadas por módulo da proteção anti-malware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

6.6.2.9.4. Em plataforma Windows, deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;

6.6.2.9.5. Deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;

6.6.2.9.6. O scan de arquivos comprimidos deve ser de no mínimo 6 camadas de compressão;

6.6.2.9.7. O scan de arquivos comprimidos do tipo OLE deve ser de no mínimo 20 camadas de compressão.

6.6.2.10. A funcionalidade de proteção contra URLs Maliciosas deve possuir as seguintes características:

6.6.2.10.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

6.6.2.10.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas.

6.6.2.11. O módulo de Firewall deve possuir as seguintes características:

6.6.2.11.1. Operar como firewall de host, através da instalação de agente nos servidores protegidos;

6.6.2.11.2. Deve possuir a capacidade de controlar o tráfego baseado nos tipos de protocolos, endereços IP e intervalo de portas.

6.6.2.12. Detecção e Resposta Avançada de Ataques (XDR):

6.6.2.12.1. Deve suportar a coleta de dados de diversas fontes, incluindo endpoints, rede, filtros da web e sensores de nuvem, para acelerar a detecção e resposta a incidentes e reduzir os tempos de resposta;

6.6.2.12.2. Deverá permitir a integração com plataformas de segurança via API;

6.6.2.13. Deve ser capaz de ingerir diversas fontes de dados, entre elas Network Intrusion Detection Systems (NIDS), Endpoint Protection Platforms (EPP), Endpoint Detection and Response (EDR), com objetivo de aprimorar o processo de detecção de ameaças e tornar ágil processo de correlação e investigação de alertas;

6.6.2.14. A quantidade de coletores necessários para a total ingestão de eventos do ambiente não deve onerar ou gerar custos adicionais de licenciamento;

6.6.2.15. Deve permitir a automação das atividades de resposta a incidentes com base nas necessidades e processos mapeados;

6.6.2.16. Deve fornecer visibilidade de possíveis vazamentos de contas de usuário;

6.6.2.17. Deve fornecer informações de elevação de privilégio das contas nos dispositivos;

6.6.2.18. Deve ser compatível com a solução NSX da VMware para permitir integração com os ambientes virtualizados;

6.6.2.19. Deverá possuir modelos pré-definidos pelo fabricante de atividades suspeitas e maliciosas para identificação e categorização de ameaças no ambiente;

6.6.2.20. Permitir criação de listas de exceção de objetos para redução de falso-positivo;

6.6.2.21. Os modelos de detecção devem possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis: crítico; alto; médio;baixo;

6.6.2.22. Deve ser possível identificar individualmente relatórios de ameaça;

6.6.2.23. Deve permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa raiz;

6.6.2.24. Deve exibir todos os detalhes do incidente em uma única página, contendo no mínimo:

6.6.2.24.1. Status do incidente;

6.6.2.24.2. Score;

6.6.2.24.3. Técnica do MITRE utilizada;

6.6.2.24.4. Modelo(s) de detecção acionado(s);

6.6.2.24.5. Objetos detectados dentro de cada modelo;

6.6.2.25. Permitir coletar e fazer o download de um arquivo para investigação local detalhada;

6.6.2.26. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;

6.6.2.27. O módulo deve ser integrado como solução do endpoint e ser gerenciado pelo mesmo console, sem que haja custo de licença adicional;

6.6.2.28. Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio).

6.6.2.29. Deverá permitir ativar e desativar o produto sem a necessidade de remoção;

6.6.2.30. Deverá possuir capacidade de identificar e bloquear, no mínimo, os seguintes tipos de ataques:

6.6.2.30.1. Denial of Service (DOS);

6.6.2.30.2. Port scanning;

6.6.2.30.3. Network Flooding.

6.6.2.31. Deverá permitir a criação de políticas de segurança personalizadas;

6.6.2.32. Deverá possuir proteção avançada contra ransomware e ataques fileless;

6.6.2.33. Capacidade de identificar e bloquear processos de criptografia em massa de arquivos;

6.6.2.34. Detecção de malwares sem arquivo (fileless) que executam apenas em memória, explorando PowerShell, WMI ou scripts maliciosos;

6.6.2.35. Deverá possuir Virtual Patching (Correção Virtual de Vulnerabilidades);

6.6.2.36. Implementar proteção imediata contra vulnerabilidades conhecidas e de dia zero, mesmo antes da aplicação de patches oficiais;

6.6.2.37. Permitir aplicar regras temporárias de mitigação enquanto a atualização de software não é possível;

6.6.2.38. Bloqueio automático de processos não autorizados que tentam ser executados em ambientes de missão crítica;

6.6.2.39. Permitir a aplicação consistente de políticas em ambientes híbridos (físico, virtual e nuvem);

6.6.2.40. Resiliência e autoproteção dos agente instalados;

6.6.2.41. O agente não poderá ser desativado ou desinstalado sem credenciais administrativas;

6.6.2.42. Proteção contra tentativas de alteração ou exclusão de arquivos críticos do software;

6.6.2.43. Escalabilidade Empresarial;

6.6.2.44. O Console Web deverá ser projetado para alta disponibilidade e balanceamento de carga.

6.6.3. ITEM 3 - DESCRIÇÃO DA SOLUÇÃO - Trend Micro - Deep Discovery Inspector Series Virtual 500

6.6.3.1. A solução deverá ser instalada de modo a detectar ameaças avançadas no ambiente, inspecionando o tráfego de rede, independente de agentes instalados;

6.6.3.2. Deve ser dimensionada para inspecionar 500 Mbps de throughput;

6.6.3.3. Funcionalidades e Requisitos específicos:

6.6.3.3.1. Deverá fornecer solução integrada de proteção contra ameaças avançadas de acordo com funcionalidades e características técnicas especificadas neste documento, contendo, no mínimo os seguintes módulos:

6.6.3.3.2. Monitoramento, Identificação, Análise e Resposta de Incidentes de Segurança;

6.6.3.3.3. Detecção de ataques direcionados;

6.6.3.3.4. Analisador virtual de ameaças;

6.6.3.3.5. Correlação de regras para detecção de conteúdo malicioso;

6.6.3.3.6. Análise de todos os estágios de uma sequência de ataques.

6.6.3.4. Serviço de monitoração e análise de ameaças digitais em rede;

6.6.3.5. Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente;

6.6.3.6. Serviço que entenda ameaça digital como a representação de um software malicioso ou ação maliciosa tal como: spyware, phishing, worms, bot, trojan, adware, network Exploit, web Exploit, Cross-site scripting, spear phishing, information stealing malware e outras ações que podem compor ataques ao patrimônio computacional do ambiente;

6.6.3.7. Visibilidade e relatório de incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos;

6.6.3.8. Análise e correlação de atividades maliciosas tais como:

6.6.3.8.1. Detecção específica de malwares conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede; Detecção de vermes de rede e de e-mail no tráfego de rede;

6.6.3.8.2. Detecção de programas de exploração de vulnerabilidades (Exploits) na rede;

6.6.3.8.3. Detecção de empacotamentos maliciosos no tráfego da rede;

6.6.3.8.4. Validação de tráfego web malicioso através de consultas a sistemas de reputação na Internet;

6.6.3.8.5. Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas.

6.6.3.9. Permitir a rápida identificação da criticidade dos eventos de segurança;

6.6.3.10. Permitir realizar pesquisas avançadas e customizadas dos incidentes de segurança através da console de gerenciamento;

6.6.3.11. Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança;

6.6.3.12. Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento;

6.6.3.13. Permitir a integração com sistemas de serviço de diretório;

6.6.3.14. Capacidade de verificar em tempo real a reputação de endereços web (URL’s);

6.6.3.15. A capacidade de análise de artefatos em sandbox pode ser realizada através de integração com serviço em nuvem do próprio fabricante;

6.6.3.16. Capacidade de criar e salvar investigações customizadas dos incidentes de segurança;

6.6.3.17. Deverá possuir pelo menos 1 (um) sensor para inspecionar o tráfego de rede de throughput de 500 Mbps de análise;

6.6.3.18. Deverá possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques;

6.6.3.19. Deverá detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP;

6.6.3.20. Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso;

6.6.3.21. Os módulos de captura de rede deverão suportar a coleta de arquivos pelo menos nos protocolos HTTP e HTTPS;

6.6.3.22. Deverá possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Bittorent, Kazaa, Blubster, e Donkey, eMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP;

6.6.3.23. Deverá possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;

6.6.3.24. Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos;

6.6.3.25. Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças;

6.6.3.26. Deverá analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS, ZIP e RAR;

6.6.3.27. A solução deve detectar ameaças do dia zero, vulnerabilidade, URL’s maliciosas;

6.6.3.28. Deverá possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;

6.6.3.29. Deverá permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações;

6.6.3.30. Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados);

6.6.3.31. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística;

6.6.3.32. Deverá possuir foco em proteção contra APTs (Advanced Persistent Threats);

6.6.3.33. Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou Switches;

6.6.3.34. Deverá permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa;

6.6.3.35. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em ponto único;

6.6.3.36. Deverá possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução;

6.6.3.37. Deverá possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;

6.6.3.38. Deverá ser capaz de identificar movimentos laterais em uma rede corporativa;

6.6.3.39. Deverá atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;

6.6.3.40. Deverá possuir interface web para busca e investigação local de incidentes;

6.6.3.41. Deverá possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;

6.6.3.42. Deverá possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets;

6.6.3.43. Deverá possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como:

consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;

6.6.3.44. Deverá possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características:

6.6.3.44.1. Resumidos;

6.6.3.44.2. Visão Geral dos Incidentes de Segurança;

6.6.3.44.3. Discriminação dos Tipos de Incidentes;

6.6.3.44.4. Top Ameaças Analisadas;

6.6.3.44.5. Top Hosts Infectados;

6.6.3.44.6. Recomendações de Segurança;

6.6.3.44.7. Executivos;

6.6.3.44.8. Deve possuir detalhes técnicos dos incidentes detectados;

6.6.3.44.9. Deve possuir estatística do tráfego analisado;

6.6.3.44.10. Deve possuir indicadores de risco do ambiente;

6.6.3.44.11. Recomendações de Segurança.

6.6.3.45. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados;

6.6.3.46. Quando detectada uma ameaça, a solução deve prover, podendo esta realizar consultas em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;

6.6.3.47. As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação;

6.6.3.48. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling;

6.6.3.49. Deverá ser capaz de detectar tentativas de scan de rede;

6.6.3.50. Deverá ser capaz de detectar propagação de malwares na rede;

6.6.3.51. Deverá ser capaz de detectar tentativas de brute-force;

6.6.3.52. Deverá ser capaz de detectar tentativas de fuga e roubo de informação;

6.6.3.53. Deverá ser capaz de detectar ameaças que se replicam na rede;

6.6.3.54. Deverá ser capaz de detectar Exploits na rede;

6.6.3.55. O Monitoramento de protocolos de comunicação deve ser feito através de appliance único (ou virtual appliance);

6.6.3.56. O console de gerenciamento deve possuir mapa mundial, onde são marcadas origens de ataques e eventos de segurança monitorados pela solução;

6.6.3.57. Deverá permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo;

6.6.3.58. Capacidade de salvar uma investigação antes de ser finalizada;

6.6.3.59. Capacidade de restaurar uma investigação para continuá-la ou consultá-la;

6.6.3.60. Capacidade de emitir relatórios baseados nas investigações;

6.6.3.61. Deverá permitir exportar sob demanda os logs em texto puro (CSV ou similar);

6.6.3.62. Deverá sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;

6.6.3.63. Deverá permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;

6.6.3.64. Deverá permitir recebimento de logs via syslog;

6.6.3.65. Deverá permitir encaminhamento de logs via syslog;

6.6.3.66. Deverá permitir receber logs de diferentes dispositivos;

6.6.3.67. Deverá possuir engine de correlação de eventos;

6.6.3.68. Deve enviar alertas via e-mail para pelo menos 10 e-mails diferentes;

6.6.3.69. Deve permitir a configuração de alarmes personalizados, com base em investigações;

6.6.3.70. O console de gerenciamento deverá ser web, apresentando alta disponibilidade de modo que na ausência da principal, o restante da solução permaneça ativa e funcionando;

6.6.3.71. O console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;

6.6.3.72. O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;

6.6.3.73. Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;

6.6.3.74. O console de gerenciamento deverá ser gerenciada por Microsoft Edge, Google Chrome e Firefox;

6.6.3.75. Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções;

6.6.3.76. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;

6.6.3.77. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;

6.6.3.78. A solução deverá ter integração com ferramentas de SIEM;

6.6.3.79. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo:

6.6.3.79.1. Computadores infectados;

6.6.3.79.2. Origem de infecções;

6.6.3.79.3. Estatísticas de ameaças;

6.6.3.79.4. Riscos potenciais de segurança;

6.6.3.79.5. Riscos de perda de informações;

6.6.3.79.6. Risco de sistema comprometido;

6.6.3.79.7. Risco de disseminação de ameaças;

6.6.3.79.8. Eventos suspeitos;

6.6.3.79.9. Infecções de malware.

6.6.3.80. Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;

6.6.3.81. Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção;

6.6.3.82. Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV.

6.6.3.83. Módulo de Detecção e Resposta

6.6.3.83.1. A solução deve ter a capacidade de integrar-se com a plataforma de investigação e resposta centralizada, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente;

6.6.3.83.2. A funcionalidade deve ser licenciada para analisar o throughput total da solução;

6.6.3.83.3. A solução deve permitir a integração dos eventos ocorridos em outros segmentos com objetivo de correlacionar os ataques na rede;

6.6.3.83.4. Deve permitir a análise em linha de tempo gráfica, representando a sequência da comunicação dos ativos, bem como seu protocolo e direção;

6.6.3.83.5. Deve identificar tentativas de ataques avançados na rede e correlacionar com eventos das soluções de estação de trabalho, servidores e e-mail, a fim de rastrear o passo-a-passo do ataque na rede;

6.6.3.83.6. Ao clicar em um dos objetos identificados pela solução de inspeção de rede, a plataforma deverá informar um resumo do ataque em questão, contendo o IP/hostname envolvido, quais protocolos, atividades maliciosas, severidade do incidente, fases do ataque;

6.6.3.83.7. A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores;

6.6.3.83.8. A solução deve possuir módulo de investigação, detecção integrados;

6.6.3.83.9. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada.

6.6.3.84. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

6.6.3.85. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

6.6.3.86. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

6.6.4. ITEM 4 - DESCRIÇÃO DA SOLUÇÃO - Horas técnica de suporte

6.6.4.1. O serviço de suporte deverá se prestado por profissionais capacitados e com certificações válidas emitidas pela Trend Micro em qualquer um dos produtos ofertados;

6.6.4.2. O serviço de suporte técnico deve contemplar todos os itens descritos na presente especificação técnica e deve considerar as seguintes soluções Trend Micro:

6.6.4.2.1. Trend Micro Endpoint Security CORE;

6.6.4.2.2. Trend Micro Endpoint Security PRO;

6.6.4.2.3. Deep Discovery Inspector;

6.6.4.2.4. Deep Security Software;

6.6.4.2.5. Trend Micro Apex One Sandbox;

6.6.4.2.6. Trend Micro Vision One;

6.6.4.3. O serviço de suporte engloba as seguintes atividades:

6.6.4.3.1. Instalação, reinstalação, configuração e reconfiguração das licenças;

6.6.4.3.2. Desinstalação, reconfiguração ou reinstalação decorrente de falhas no software;

6.6.4.3.3. Atualização de versão de software disponibilizada pelo fabricante da solução;

6.6.4.3.4. Correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

6.6.4.3.5. Transferência de conhecimento;

6.6.4.3.6. Coadministração da ferramenta;

6.6.4.3.7. Atendimento a incidentes de qualquer natureza e em qualquer uma das soluções ofertadas;

6.6.4.3.8. Interface com o fabricante para novas funcionalidades e ameaças;

6.6.4.3.9. Configuração e adequação das ferramentas ao ambiente;

6.6.4.4. O serviço de suporte técnico deverá ser realizado em duas modalidades:

6.6.4.4.1. Remoto: telefônico ou via internet, a ser disponibilizado em horário comercial e/ou fora deste dependendo da criticidade do evento pelo qual foi aberto chamado;

6.6.4.4.2. On-site: a ser efetuado nas instalações da PMC;

6.6.4.5. Para atendimento remoto via telefone, a provedora dos serviços de suporte deverá disponibilizar número telefônico local, com DDD da Região Metropolitana do de Porto Alegre caso contrário deverá ser um número de atendimento telefônico gratuito (0800);

6.6.4.6. Os serviços de atendimento on-site poderão ser solicitados tanto pela internet quanto por telefone;

6.6.4.7. As horas correlacionadas só serão consumidas em caso de abertura de chamado;

6.6.4.8. Todas as solicitações feitas pela PMC, em qualquer das modalidades de atendimento descritas acima, deverão ser registradas em sistema informatizado para acompanhamento e controle da execução dos serviços;

6.6.4.9. Para registro e acompanhamento dos chamados via internet, este sistema deverá disponibilizar interface de acesso web, com autenticação de usuário por meio de login e senha.

6.7. PRAZO E VIGÊNCIA DO CONTRATO

6.7.1. O prazo de vigência do contrato será de 12 (doze) meses, podendo ser prorrogáveis por novos períodos até o limite legal;

6.7.2. Devem estar incluídos todos os custos relacionados à prestação dos serviços, além de despesas diretas e indiretas, tais como: salários, encargos sociais, fiscais, tributários, trabalhistas, previdenciários, indenizações e quaisquer outras que forem devidas aos seus empregados ou prepostos na execução dos serviços objeto do contrato; deslocamento, hospedagem, transporte e alimentação de pessoal, transporte de equipamentos e materiais, fretes,

seguros, garantia, custos com impressões, entre outros. Impostos, taxas, fretes ou outras despesas se houver.

6.8. REQUISITOS DO NEGÓCIO

6.8.1. Solução de segurança para endpoint: é um software projetado para proteger dispositivos finais, como computadores, laptops e dispositivos móveis, contra uma variedade de ameaças digitais, incluindo malware, ransomware, phishing e outras formas de ataques cibernéticos. Essas soluções geralmente incluem recursos como antivírus, firewall, detecção de intrusão, controle de aplicativos e proteção de dados, visando garantir a integridade, confidencialidade e disponibilidade dos dados armazenados nos dispositivos e na rede corporativa.

6.8.2. Solução de segurança para servidores físicos e virtuais: é um conjunto integrado de medidas e ferramentas destinadas a proteger os ativos de uma organização em ambientes de TI diversos. Essas soluções devem adaptar-se às peculiaridades de cada tipo de infraestrutura, garantindo a proteção de servidores físicos contra acessos não autorizados e ataques físicos, a segurança de servidores virtuais contra ameaças digitais e a integridade dos dados e aplicações contidos nestas infraestruturas;

6.8.3. Considerando o atual cenário de ciberameaças, observa-se que agentes maliciosos vêm utilizando de forma crescente recursos de **Inteligência Artificial (IA)** para potencializar e acelerar seus ciclos de ataque. O emprego de tecnologias de automação ofensiva tem resultado em menor latência para a execução das ações ilícitas e, consequentemente, em um tempo reduzido de violação (Time to Breach – TTB), o que aumenta de forma significativa a taxa de sucesso das investidas cibernéticas; Diante desse contexto, as equipes de segurança da informação necessitam adotar estratégias defensivas que contemplem **automação avançada e monitoramento contínuo**, por meio de ferramentas modernas de prevenção, detecção e resposta a incidentes, aliadas a processos devidamente estruturados e validados.

A utilização de solução integrada de segurança, com módulos de **IA baseados em análise comportamental**, permitirá à Administração ampliar a estabilidade, a disponibilidade e a resiliência de sua infraestrutura tecnológica, reduzindo riscos de indisponibilidade e comprometimento dos sistemas de missão crítica.

Do ponto de vista econômico, destaca-se ainda a necessidade de **otimização do custo total de propriedade (TCO)**, por meio da consolidação de uma solução única e integrada de detecção e resposta a ameaças, evitando a fragmentação em múltiplas ferramentas isoladas e assegurando maior eficiência operacional.

A contratação também se alinha ao princípio da melhoria contínua dos processos de segurança, buscando fortalecer a atuação preventiva, aprimorar a capacidade de identificação de comportamentos anômalos e acelerar a resposta a incidentes, elevando a percepção de segurança junto aos usuários e demais partes interessadas da Administração Pública.

No âmbito da presente contratação, a estratégia de segurança da informação está estruturada em **cinco fases do ciclo de proteção cibernética**, a seguir descritas:

I - Prevenção: ações voltadas à mitigação de ameaças, com foco em impedir a infiltração de agentes maliciosos na rede e classificar ataques direcionados em tempo real, de modo a interromper o vetor de ataque antes de sua execução;

II - Detecção: esforços destinados ao reconhecimento e identificação de ameaças que, apesar das medidas preventivas, tenham alcançado a infraestrutura tecnológica, abrangendo estações de trabalho, servidores e rede.

III - Contenção: procedimentos para impedir a disseminação da ameaça cibernética identificada, restringindo seu alcance e efeitos.

IV - Recuperação: fase subsequente à contenção, destinada à restauração da infraestrutura de TI ao seu estado anterior estável e seguro, com eventual melhoria em sua configuração.

V - Remediação: medidas voltadas à atualização de processos e tecnologias para prevenir reincidências, incluindo reforço de programas de capacitação e conscientização dos usuários, reconhecendo a importância do fator humano na redução de riscos de violações.

6.9. REQUISITOS DE CAPACITAÇÃO

6.9.1. Todos os serviços a serem executados no âmbito do presente contrato, sejam eles prestados diretamente pela empresa contratada ou pelo fabricante da solução, durante todo o período de vigência contratual, deverão ser realizados por **analistas e/ou técnicos devidamente qualificados e certificados** nas ferramentas objeto da contratação, assegurando a correta execução das atividades e a plena eficácia da solução adquirida.

6.10. REQUISITOS TEMPORAIS

6.10.1. Os serviços contratados deverão ser prestados pelo período de 12 (doze) meses, prorrogáveis conforme legislação vigente;

6.10.2. O prazo para a entrega dos itens é de 30 (trinta) dias corridos após a emissão da Ordem de Início dos Serviços (OIS);

6.10.3. Os componentes das soluções serão recebidos provisoriamente no prazo de até 15 (quinze) dias corridos, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta;

6.10.4. Os componentes das soluções poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 30 (trinta) dias corridos, a contar da notificação à CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades;

6.10.5. Os componentes das soluções serão recebidos definitivamente no prazo de até 15 (quinze) dias corridos, contados do recebimento provisório, após a verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta;

6.10.6. Na hipótese da verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo, exceto no caso de não conformidade dos itens fornecidos com as especificações constantes no Termo de Referência e na proposta;

6.10.7. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato;

6.10.8. Os serviços de console de gerenciamento deverão estar disponíveis 90% no mês, minimamente;

6.10.9. A solução da CONTRATADA deverá garantir a detecção e remoção programas maliciosos como spyware, programas de propaganda, ferramentas como password crackers, etc., para os servidores e para os desktops, de forma automática, em pelo menos 90,00% (noventa por cento) dos casos. Para os casos em que a solução não remova a infecção automaticamente, o fabricante da solução deverá fornecer ferramenta disponível para tal ação de reparação;

6.10.10. A solução deverá garantir a atualização automática das assinaturas de antivírus em pelo menos 90% (noventa por cento) das estações e servidores ativos e disponíveis na rede em até no máximo 24 (vinte e quatro) horas após o recebimento desta pelo servidor. Para os casos em que a solução não atualize automaticamente as assinaturas de antivírus, a solução deverá fornecer formas de fazer as atualizações de forma manual;

6.10.11. Os atendimentos de suporte técnico e/ou consultoria prestados à CONTRATANTE deverão pautar-se pelas instruções abaixo:

6.10.12. caso seja on-site, o atendimento deverá ser provido na sede da Prefeitura Municipal de Canoas e/ou Canoastec.

6.10.13. remoto, deverá ser realizada abertura de chamado técnico para verificação da ocorrência ou necessidade de consultoria, devendo o prazo de atendimento em horas contar a partir do atendimento junto ao CONTRATANTE.

6.11. REQUISITOS DE SEGURANÇA E PRIVACIDADE

6.11.1. A CONTRATADA deverá manter sob sigilo as informações e comunicações de que ver conhecimento, abstendo-se de divulgá-las, garantindo o sigilo e a inviolabilidade dos dados trafegados por meio dos enlaces eventualmente utilizados na execução das atividades, respeitando as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações;

6.11.2. A CONTRATADA não poderá armazenar consigo qualquer documento técnico que contemple configurações aplicadas nos equipamentos implantados na rede da CONTRATANTE de forma que identifique credenciais e/ou ativos de redes interno;

6.11.3. A CONTRATADA deverá informar à CONTRATANTE todas as senhas utilizadas para a configuração dos equipamentos, as quais deverão ser alteradas pela CONTRATANTE com o apoio técnico da CONTRATADA, logo após o encerramento do contrato ou sempre que a CONTRATANTE julgar necessário;

6.11.4. A CONTRATADA deverá prover segurança de acesso físico e lógico aos recursos da CONTRATANTE que estiverem sob sua guarda;

6.11.5. Os recursos de TI não poderão ser utilizados pela CONTRATADA ou seus prepostos para realização de atividades alheias aos serviços previstos ou englobados nesta contratação;

6.11.6. A CONTRATADA deverá guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual manda com a PMC, abstendo-se de divulgá-los a terceiros sob qualquer pretexto, a menos que prévia e formalmente autorizada pela CONTRATANTE;

6.11.7. Todos os perfis de acesso concedidos à CONTRATADA deverão ser imediatamente excluídos após o término do contrato;

6.11.8. A CONTRATANTE terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

6.11.9. A CONTRATADA deverá respeitar as normas de segurança estabelecidas pela CONTRATANTE durante a realização de atividades no ambiente

desta. Essa sujeição não caracteriza qualquer vínculo empregatício com a CONTRATANTE;

6.11.10. Deverão ser adotadas, sempre que possível, as versões mais recentes dos softwares básicos do ambiente da CONTRATANTE.

7. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS:

Item	Descrição do item	Nº da licença	Unidade	Quantidade
1	Trend Micro - Endpoint Security CORE	VORA0029	UND	4000
2	Trend Micro - Endpoint Security PRO	VORA0042	UND	150
3	Trend Micro - Deep Discovery Inspector Series Virtual 500	DDNA0036	UND	1
4	Horas técnica de suporte		HORA	400

7.1. Os quantitativos estimados, bem como a modalidade de contratação pretendida escolhida, tem como princípios o interesse público, oportunidade e conveniência, pois a modalidade escolhida permite com que a Prefeitura Municipal de Canoas possa gerir de forma coesa e coerente com os aspectos relacionados à tecnologia da informação e comunicação, com foco no interesse coletivo e utilidade pública, provendo soluções inovadoras e sustentáveis.

7.2. Atualmente, o Município possui aproximadamente 2.500 (dois mil e quinhentos) computadores integrados ao domínio institucional (Active Directory), ambiente centralizado de autenticação e gerenciamento dos equipamentos corporativos, que constituem a base do parque computacional atualmente protegido.

Adicionalmente, há previsão de ampliação do uso de solução nas unidades escolares do Município, estimando-se inicialmente cerca de 300 (trezentos) computadores em laboratórios e setores administrativos das escolas, bem como, a inclusão de parte dos equipamentos disponibilizados para uso pedagógico por professores, conforme evolução do processo de padronização e integração desses ambientes à gestão corporativa de TI.

Os quantitativos previstos também contemplam pequena margem técnica de segurança, estimada entre 50 (cinquenta) e 100 (cem) licenças, destinada a absorver variações naturais do ambiente, tais como: substituição de equipamentos, novas aquisições ou necessidade de proteção de ativos incorporados durante a vigência contratual, evitando descontinuidade de cobertura.

Quanto às licenças destinadas a servidores e máquinas virtuais, o dimensionamento foi realizado considerando exclusivamente o ambiente de produção, responsável pela execução dos sistemas e serviços institucionais críticos, contemplando ainda, variações operacionais decorrentes da criação, substituição ou expansão de máquinas virtuais necessárias à continuidade dos serviços públicos.

Dessa forma, os quantitativos previstos refletem o ambiente, atualmente, em operação e sua expansão planejada, assegurando cobertura adequada dos ativos institucionais e continuidade da proteção do ambiente tecnológico municipal.

8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO:

8.1. Considerando a INSTRUÇÃO NORMATIVA SEGES/ME No 65, DE 7 DE JULHO DE 2021, estabelecemos que a estimativa de valor da presente contratação foi estabelecida a partir de pesquisa de preços, considerando esse Estudo Técnico em questão.

8.2. A IN aponta como formas de pesquisa de preços a:

8.2.1. “composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente”;

8.2.2. “contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente” - foram realizados levantamentos de contratações similares, conforme se observa o estudo;

8.2.3. “dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso”;

8.3. Durante a análise deste Estudo Técnico Preliminar, identificamos valores preliminares para os itens dos objetos, que apresentam consistência significativa para a tomada de decisão por parte dos gestores da contratação;

8.4. Posteriormente, por meio de pesquisa pública de preços, realizada de acordo com a Instrução Normativa no 73/2020, do Ministério da Economia, sendo o método para obtenção do preço estimado o menor dos valores obtidos na pesquisa de preços sobre um conjunto de três ou mais preços, oriundos de um ou mais dos parâmetros de que trata o art. 5o da referida IN 73/2020;

8.5. Para o cálculo foi utilizada a “mediana de valores”, que consiste em realizar uma avaliação crítica dos preços obtidos na pesquisa, a fim de descartar valores que apresentem grandes variações em relação aos demais, conforme orientação do TCU;

8.6. Foram obtidos orçamentos diretos através de pesquisa realizada no Banco de Preços de compras públicas em 2024 e 2025, além de acesso aos sítios de internet do LicitaCon e demais órgãos das administrações públicas municipal e federal;

Item	Descrição do item	Nº da licença	Unidade	Quantidade	Valor máximo aceitável
1	Trend Micro - Endpoint Security CORE	VORA0029	UND	4000	R$ 75,19
2	Trend Micro - Endpoint Security PRO	VORA0042	UND	150	R$ 1.536,18
3	Trend Micro - Deep Discovery Inspector Series Virtual 500	DDNA0036	UND	1	R$ 164.999,06
4	Horas técnica de suporte		HORA	400	R$ 425,67

9. QUALIFICAÇÃO TÉCNICA

9.1. Declaração emitida pelo fabricante da solução objeto deste edital, estabelecendo que a proponente tenha plenas condições técnicas que assegure o atendimento e suporte técnico especializado aos produtos, licenças e serviços licitados durante todo o prazo de contratação. Esta declaração é obrigatória, já que é atendida por vários fornecedores do mercado e visa unicamente garantir a PMC a qualidade e operacionalidade dos produtos e serviços com total anuência do fabricante da solução, garantindo pleno cumprimento das cláusulas aqui estabelecidas;

9.2. Comprovação de aptidão no desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação – Atestado(s) de Capacidade Técnica, fornecido(s) por pessoa jurídica de direito público ou privado, que comprove que a Licitante executa satisfatoriamente atividades de prestação de serviço referente a suporte técnico nos softwares Trend Micro deste escopo por período não inferior a 01 (um) ano;

9.3. A CONTRATADA deverá comprovar que possui em seu quadro funcional, no mínimo, 1 (um) profissional com certificação Trend Micro, Trend Micro Vision One, Professional e/ou Trend Micro Workload Security Professional para a prestação de serviços exigidos, a CONTRATADA deverá apresentar os certificados

de formação oficial do fabricante, bem como sua relação funcional com a CONTRATADA.

10. JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA SOLUÇÃO:

10.1. Compete à administração buscar o menor dispêndio possível de recursos, assegurando a qualidade da aquisição e/ou da prestação do serviço, o que exige a escolha da solução mais adequada e eficiente dentre as diversas opções existentes já por ocasião da definição do objeto e das condições da contratação, posto que é essa descrição que impulsiona a seleção da proposta mais vantajosa;

10.2. Neste sentido, esclarecemos que nossa análise aponta para o NÃO PARCELAMENTO do objeto. Uma vez que quando reparamos o conjunto de itens especificados, especialmente no que concerne aos requisitos de qualificação técnica e desempenho necessário para o atendimento dos serviços, detalhados no Termo de Referência, no qual constam os métodos objetivos de mensuração de entregas, foram objetivamente definidos por meio de especificações usuais praticadas no mercado e representa a real demanda da CONTRATANTE, razão pela qual pode ser adotado o critério de MENOR PREÇO GLOBAL para o julgamento objetivo das propostas;

10.3. Uma vez que os atestados técnicos pedem que a empresa comprove possuir expertise no fornecimento de licenciamentos e serviços prestados, estamos respeitando a boa regra no sentido de buscar que a empresa tenha adequado nível de especialização para execução do item de maior relevância, sendo assim não se comprova no caso em tela, pelas medidas adotadas pela administração que técnica e econômica viável na vantajosidade de tal parcelamento do objeto;

10.4. Ainda sob a perspectiva técnica, impende lançar luzes sobre a centralização da responsabilidade em uma única empresa contratada, a qual consideramos adequada não apenas em vista do acompanhamento de problemas e soluções, capacitação e transferência do conhecimento, mas mormente em termos de facilitar a verificação das suas causas e atribuição de responsabilidade, de modo a aumentar o controle sobre a execução dos objetos licitados;

10.5. É cediço que a regra é o parcelamento do objeto, cujo objetivo é o de melhor aproveitar os recursos disponíveis no mercado e ampliar a competitividade, mas é imprescindível que se estabeleça que a divisão do objeto seja técnica e economicamente viável. Do contrário, existindo a possibilidade de risco ao conjunto do objeto pretendido, não há razão para fragmentar inadequadamente as aquisições e os serviços a serem contratados. Por fim, registramos que se trata de um objeto complexo e indivisível, mas de objetos com elementos técnicos e econômicos do caso concreto condizem com o seu não-parcelamento.

11. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES:

11.1. Trata-se de uma visão global do órgão ou entidade pública com vistas a identificar se existem em andamento contratações correlatas ou interdependentes que venham

a interferir ou merecer maiores cuidados no planejamento da futura contratação;

11.2. Contratações correlatas são aquelas que guardam relação com o objeto principal, interligando-se a essa prestação do serviço, mas que não precisam, necessariamente, ser adquiridas para a completa prestação do objeto principal;

11.3. Já as contratações interdependentes são aquelas que precisam ser contratadas juntamente com o objeto principal para sua completa prestação;

11.4. No caso concreto, não se verificam contratações correlatas nem interdependentes para a viabilidade e contratação desta demanda.

12. DEMONSTRATIVO DA PREVISÃO DA CONTRATAÇÃO NO PLANO ANUAL DE CONTRATAÇÃO – PAC:

12.1. A previsão da contratação possui alinhamento com o planejamento da Administração Pública Municipal de Canoas.

13. DEMONSTRAÇÃO DOS RESULTADOS PRETENDIDOS:

13.1. Com a contratação da solução de segurança propostos neste Estudo Técnico Preliminar, pretende-se alcançar os seguintes resultados:

13.1.1. Fortalecimento da postura de cibersegurança institucional, assegurando proteção contínua contra malwares, ransomwares, ataques direcionados e demais ameaças avançadas que possam comprometer a infraestrutura tecnológica;

13.1.2. Mitigação de riscos operacionais e de indisponibilidade, por meio da detecção proativa e resposta rápida a incidentes, reduzindo a probabilidade de interrupção de serviços essenciais prestados pela Administração;

13.1.3. Padronização e centralização do gerenciamento da segurança, possibilitando à equipe técnica monitorar e aplicar políticas de proteção de forma uniforme em todos os endpoints, servidores e estações de trabalho, com relatórios de auditoria e rastreabilidade das ações;

13.1.4. Atendimento a requisitos legais e normativos, incluindo as melhores práticas de governança em Tecnologia da Informação e Comunicação (TIC), observando os princípios da economicidade, eficiência e continuidade do serviço público;

13.1.5. Redução do tempo médio de resposta a incidentes (MTTR), por meio da integração da solução com ferramentas de XDR (Extended Detection and Response) e recursos avançados de correlação de eventos;

13.1.6. Maior resiliência cibernética, garantindo que a Administração possa cumprir suas funções institucionais mesmo diante de cenários de ataque ou tentativa de exploração de vulnerabilidades.

14. MATRIZ DE RISCOS

14.1. Em atendimento ao disposto no art. 18, inciso VII, da Lei nº 14.133/2021, bem como às orientações da Instrução Normativa SEGES/ME nº 58/2022, apresenta-se a avaliação de riscos inerentes à presente contratação;

14.2. A análise de riscos busca identificar, classificar e propor medidas de tratamento para eventos que possam comprometer os objetivos da contratação, seja sob a ótica técnica, administrativa, financeira ou operacional;

14.3. A matriz de riscos, a seguir, sintetiza os principais fatores que podem impactar a execução do objeto, atribuindo-lhes níveis de probabilidade e impacto, bem como as estratégias de mitigação correspondentes. Ressalta-se que a avaliação foi elaborada com base nas melhores práticas de gestão de riscos da Administração Pública, de forma a assegurar maior governança, previsibilidade e eficiência na execução contratual;

Risco Identificado	Descrição	Probabilidade	Impacto	Consequência	Medidas Mitigatórias	Responsável
Incompatibilidade técnica	A solução contratada não se integra adequadamente com a infraestrutura existente (servidores, endpoints, rede).	Média	Alto	Interrupção de serviços e retrabalho de configuração	Realizar análise prévia de compatibilidade pela área de TI; solicitar PoC (Prova de Conceito) ou ambiente piloto.	Área Técnica Fornecedor
Subdimensionamento de licenças	Número de licenças adquiridas insuficiente para atender ao parque tecnológico atual ou crescimento futuro.	Média	Alto	Usuários/ servidores desprotegidos, expondo o ambiente a riscos	Levantamento detalhado do inventário de ativos; prever margem de crescimento em contrato.	Área Técnica Contratante
Atraso na entrega implantação	Fornecedor não cumpre prazo de disponibilização da solução ou instalação.	Baixa	Alto	Comprometimento da continuidade do serviço de segurança	Definir cronograma contratual claro; penalidades por descumprimento; acompanhamento pela fiscalização.	Fornecedor Contratante
Obsolescência tecnológica	Evolução rápida das ameaças e tecnologias pode tornar a solução insuficiente durante o contrato.	Média	Alto	Redução da efetividade da proteção e necessidade de aditivo	Contratar solução reconhecida em relatórios de mercado (Gartner, Forrester); prever cláusula de atualização de versão sem custo adicional.	Área Técnica Contratante
Variação de custos futuros	Reajustes inesperados em renovações de licenciamento.	Alta	Médio	Elevação de custos e dificuldade de continuidade contratual	Previsão orçamentária plurianual; cláusulas contratuais de reajuste limitadas por índices oficiais (IPCA).	Setor Financeiro Contratante

Falhas de suporte técnico	Atendimento deficiente por parte do fornecedor em incidentes críticos.	Baixa	Alto	Prolongamento de indisponibilidade e aumento de impacto operacional	Exigir SLA de atendimento e resolução; acompanhar indicadores em relatórios de desempenho.	Fornecedor / Contratante
Vazamento de dados	Configuração incorreta ou falha na solução pode gerar exposição de informações sensíveis.	Baixa	Alto	Quebra de sigilo, responsabilização legal e danos à imagem institucional	Configuração validada por equipe especializada; auditorias periódicas; logs de auditoria obrigatórios.	Área Técnica Contratante
Resistência de usuários	Dificuldade de adaptação a políticas de bloqueio e controle implementadas.	Média	Médio	Tentativas de burlar o sistema e queda de produtividade inicial	Capacitação e comunicação prévia com usuários; criação de listas de exceção controladas.	Área Técnica Gestão de Pessoas
Dependência de único fabricante	Forte dependência tecnológica da Trend Micro para continuidade da proteção.	Alta	Médio	Redução de alternativas futuras e risco de dependência financeira operacional	Registrar comparativo de mercado no ETP; manter documentação que comprove escolha vantajosa	Área Técnica Contratante

15. PROVIDÊNCIAS PRÉVIAS AO CONTRATO:

15.1. Para assegurar a correta instrução do processo e a aderência à legislação vigente, deverão ser observadas as seguintes providências antes da formalização do contrato:

15.1.1. Realização de Estudo Técnico Preliminar (ETP), já em andamento, que subsidia a necessidade administrativa e demonstra a motivação da contratação;

15.1.2. Análise de Riscos, identificando potenciais impactos de não contratação ou da contratação inadequada, e propondo medidas mitigadoras que assegurem a efetividade da solução;

15.1.3. Pesquisa de preços, em conformidade com a Instrução Normativa vigente, incluindo consultas a contratações similares em outros órgãos da Administração, bem como orçamentos de fornecedores, para garantir a vantajosidade da proposta;

15.1.4. Definição do modelo de execução contratual, especificando se a solução será adquirida como licenciamento perpétuo, assinatura anual ou outro regime aplicável, em consonância com as regras de orçamento e planejamento de TIC;

15.1.5. Parecer técnico da área de TI, confirmando a compatibilidade da solução com a infraestrutura existente e recomendando sua adoção como forma de continuidade das políticas de segurança já implantadas;

15.1.6. Previsão orçamentária, com a devida dotação aprovada, garantindo recursos para a contratação e manutenção da solução durante a vigência do contrato;

15.1.7. Publicação do extrato do edital, garantindo a publicidade e a observância ao princípio da transparência.

16. PLANEJAMENTO E POSSÍVEIS IMPACTOS AMBIENTAIS:

16.1. Não se apresentam critérios específicos de sustentabilidade para a proposta em tela. Contudo, aponta-se a importância da observação dos requisitos definidos nos Guias de Licitações Sustentáveis da Advocacia Geral da União (AGU) - Guia Nacional de Licitações Sustentáveis - NESLIC e Guia Prático de Licitações Sustentáveis - 3a Edição - disponíveis em http://www.agu.gov.br/page/content/detail/id_conteudo/138067, sempre que aplicável;

16.2. Para além de recursos ambientais, a contratada deve observar práticas que garantam os direitos trabalhistas, de respeito à raça, cor, sexo, orientação sexual ou estado civil.

17. VIABILIDADE DA CONTRATAÇÃO:

17.1. Após a análise contida neste Estudo Técnico Preliminar, a recomendação técnica da CanoasTec para contratação dos serviços ora denominados neste documento, portanto, acarretando menor investimento o qual se mostra como opção com maior vantagem comparativa em eficiência, economicidade e garante a prestação dos serviços de forma adequada e resiliente.

gov.br Documento assinado digitalmente
GUILHERME DIONIER GASPARETTO
Data: 20/02/2026 12:00:51-0300
Verifique em https://validar.iti.gov.br

Nome: Guilherme Dionier Gasparetto
Matrícula: 161
Diretoria de Infraestrutura - CanoasTec

BRAULIO PIRES PONTES JUNIOR
Assinado de forma digital por BRAULIO PIRES PONTES JUNIOR
Dados: 2026.02.20 12:39:20 -03'00'

Nome: Braulio Pires Pontes Junior
Matrícula: 162
Diretoria de Infraestrutura - CanoasTec

Vanessa Fraga da Rocha
Matrícula 128074
Secretária Municipal de Administração