ESTUDO TÉCNICO PRELIMINAR - ETP SEI Nº 27711447/2025 - SAP.UGC

1 - DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (obrigatório)

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, este campo é obrigatório.

O ambiente digital enfrenta um crescimento exponencial no número e na complexidade das ameaças cibernéticas. Ransomwares, malwares avançados, ataques de dia zero, engenharia social e outras técnicas maliciosas têm se tornado cada vez mais frequentes, atingindo tanto o setor privado quanto o setor público. Tais incidentes podem comprometer informações sigilosas, causar paralisações operacionais, prejuízos financeiros e danos à imagem institucional.

Diante desse cenário, soluções de segurança tradicionais - baseadas exclusivamente em assinaturas - têm se mostrado insuficientes para enfrentar ameaças modernas, que frequentemente são inéditas, persistentes e adaptáveis.

Nesse sentido, a contratação de serviços de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint**)** evolui o conceito de antivírus tradicional ao oferecer um conjunto de funcionalidades voltadas à:

- Detecção comportamental de ameaças em tempo real.
- Resposta automatizada a incidentes.
- Isolamento de máquinas infectadas para evitar propagação.
- Coleta de dados e logs para análise forense.
- Visibilidade completa dos endpoints da rede.

Dessa forma, o EDR transforma o processo de proteção de endpoints (estações de trabalho, notebooks e servidores) em uma abordagem proativa, com monitoramento contínuo e capacidade de resposta imediata, mesmo diante de ameaças desconhecidas.

São benefícios esperados dessa contratação:

- **Detecção avançada de ameaças**: A tecnologia EDR oferece mecanismos de detecção baseados em comportamento e inteligência artificial, capazes de identificar ataques sofisticados, como ransomwares, malwares polimórficos e ameaças de dia zero, que geralmente não são identificadas por soluções tradicionais de antivírus.
- **Resposta automatizada e contenção de incidentes**: A solução permite a resposta automatizada a eventos suspeitos, com ações como isolamento de endpoints, encerramento de processos maliciosos e remoção de arquivos comprometidos. Isso reduz significativamente o tempo de reação e os impactos operacionais decorrentes de incidentes de segurança.
- **Visibilidade e monitoramento centralizado**: Com um painel de controle unificado, a solução proporciona visibilidade contínua de todos os endpoints da rede, permitindo a análise de comportamento, detecção de anomalias e monitoramento em tempo real das ameaças.
- **Redução do risco de vazamento de dados**: A solução contribui diretamente para a proteção de dados sensíveis e estratégicos, reduzindo o risco de acessos não autorizados, sequestro de informações e exfiltração de dados.
- **Análise forense e suporte à auditoria**: A funcionalidade de EDR inclui coleta e armazenamento de logs detalhados de eventos relacionados à segurança, possibilitando análise forense posterior, auditoria de conformidade e aprimoramento contínuo das políticas de segurança da informação.
- **Alta disponibilidade e continuidade dos serviços**: Ao mitigar de forma proativa incidentes de segurança, a solução contribui para a estabilidade dos serviços digitais da instituição, evitando interrupções, perdas de produtividade e danos à imagem institucional.
- **Integração com ecossistemas de segurança**: A solução pode ser integrada a ferramentas complementares como firewalls, sistemas de prevenção de intrusão (IPS/IDS), soluções de backup e plataformas de gerenciamento de eventos e informações de segurança (SIEM), fortalecendo a abordagem de segurança em camadas.

Ademais, destacamos que a contratação de empresa especializada na prestação de serviços de antivírus e antimalware com EDR (Detecção e Resposta de Endpoint) está amparada por fundamentos legais e boas

práticas, tais como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que exige a adoção de medidas técnicas e administrativas adequadas para a proteção de dados pessoais, sob pena de sanções legais, o Marco Civil da Internet (Lei nº 12.965/2014), que estabelece a responsabilidade dos gestores públicos quanto à proteção da integridade dos dados e dos sistemas utilizados, além de atender boas práticas internacionais de segurança da informação, como as preconizadas pela ISO/IEC 27001:2022 e pelo framework NIST.

Atualmente, a Administração Pública Municipal possui o Termo de Contrato Nº 369/2024 (SEI 0020173638) vigente, o qual terá sua execução encerrada em 01/03/2026. A ausência de solução de antivírus ou a utilização de antivírus desatualizado ou obsoleto representa um risco grave e pode ocasionar diversos danos à administração pública, sendo que a contratação vista mitigar os seguintes riscos:

- Vazamento de Dados: Roubo e exposição de informações confidenciais de cidadãos, como dados pessoais, documentos e histórico de serviços.
- Perda de Acesso a Sistemas (Ransomware): Ciberataques como o ransomware podem bloquear o acesso a sistemas essenciais, paralisando serviços públicos críticos como a folha de pagamento, emissão de documentos e gestão de tributos.
- Perda de Informações: Vírus e malwares podem corromper ou apagar dados importantes, resultando em retrabalho e interrupção na prestação de serviços.
- Prejuízo Financeiro: Custos altos para recuperação de sistemas, potencial pagamento de resgates, multas por vazamento de dados e perda de produtividade, impactando negativamente o orçamento público.
- Danos à Credibilidade: Perda de confiança da população na capacidade da gestão municipal de proteger seus dados.

Diante o exposto e considerando os riscos crescentes no ambiente digital e da necessidade de proteger os sistemas e dados institucionais, a contratação de empresa especializada na prestação de serviços de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint), não é apenas recomendável, mas essencial. Trata-se de uma medida estratégica e necessária para garantir a integridade, disponibilidade e confidencialidade das informações, bem como a continuidade das operações realizadas pela Prefeitura de Joinville.

2 – DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL.

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, em caso do não preenchimento deste campo, devem ser apresentadas as devidas justificativas.

A possibilidade de dispensar-se a elaboração do Plano de Contratações Anual - PCA vem sendo objeto de estudo da doutrina especializada, podendo ser encontradas manifestações no sentido de ser viável ou inviável a sua inexigência.

Na esfera municipal, a temática é abordada na Instrução Normativa nº 03/2024 (0023970042), aprovada pelo Decreto nº 64.109/2024 (0023987931), que prevê:

> Art. 9º. O Plano de Contratações Anual - PCA **poderá** ser exigido a partir do exercício de 2024, caso em que os Documentos de Formalização de Demanda deverão ser encaminhados até 01 de abril de 2023.

Ademais, a Circular SEI n.º 0020642825 / 2024 - SAP.ARC, traz ainda que "[...] Para o ano de 2025 não será exigido o encaminhamento das demandas para elaboração do Plano de Contratações Anual até 01/04/2024. O calendário para fins de elaboração do Plano de Contratações Anual para os próximos exercícios, será apresentado pela Secretaria de Administração e Planejamento em momento oportuno, após verificação do melhor procedimento". Informamos que, até o momento, não houve manifestação neste sentido.

Outrossim, a presente contratação está contemplada no Plano Plurianual 2026-2029 do Município de Joinville (SEI 26758096), em seu Anexo II – Valores por Unidades Orçamentárias, Ações e Metas (SEI 26451531). A despesa decorrente da contratação está prevista na Lei N.º 9.782/2024 (SEI 0023982275), que estabelece a Lei Orçamentária Anual (LOA) para o ano 2025, conforme Anexo H - Balancete Orçamentário - Detalhamento da Despesa (SEI 0023885274), e tabela a seguir:

Órgão	Despesa	Natureza	Página LOA 2025 (SEI nº 0023885274)
Secretaria de Administração e Planejamento – SAP	246/2025	3.3.90	4
Secretaria da Saúde – SES	256/2025 257/2025 308/2025 309/2025 50/2025	3.3.90	49 e 50
	597/2025 5982025 5992025 603/2025 639/2025 651/2025 652/2025 653/2025 661/2025 662/2025 663/2025 929/2025 930/2025 932/2025 937/2025	3.3.90	

Secretaria de Educação – SED	938/2025 963/2025 1004/2025 1005/2025		8, 10, 11, 14, 17, 18
Departamento de Trânsito de Joinville (DETRANS)	523/2025	3.3.90	70
Hospital Municipal São José – HMSJ	393/2025 394/2025 395/2025 398/2025	3.3.90	56

A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

3 – REQUISITOS DA CONTRATAÇÃO

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, em caso do não preenchimento deste campo, devem ser apresentadas as devidas justificativas.

Para adequada satisfação da necessidade da Administração, devem ser atendidos os seguintes requisitos mínimos:

3 Requisitos Técnicos

3.1 Requisitos Técnicos Funcionais

3.1.1 Proteção Endpoint: Solução unificada com capacidades de prevenção e detecção/resposta;

3.1.2 Console Centralizado: Interface web única para gerenciamento de toda infraestrutura;

3.1.3 Compatibilidade: Suporte a Windows, Linux, *macOS* e ambientes virtualizados;

3.1.4 Inteligência Artificial: Capacidade de detecção de ameaças *zero-day* por comportamento;

3.1.5 Integração: APIs abertas para integração com SIEM e outras ferramentas de segurança;

3.1.6 Demais requisitos serão pormenorizados no Termo de Referência e Anexo I - Especificações Técnicas.

3.2 Requisitos de Performance

3.2.1 Disponibilidade do serviço: ≥ 99,0% *uptime* do serviço;

3.2.2 Capacidade: Suporte para 20.000 *endpoints* simultâneos;

3.2.3 Latência: Impacto máximo de 5% na performance dos dispositivos protegidos;

3.2.4 Demais requisitos serão pormenorizados no Termo de Referência.

3.3 Requisitos de Suporte Técnico

3.3.1 A Solução deverá incluir suporte técnico, de manutenção dos tipos preventiva, corretiva e adaptativa, bem como atualizações.

3.3.2 A CONTRATADA deverá disponibilizar uma ferramenta eletrônica de registro de solicitação de serviços, configurável, para os níveis mínimos de serviços exigidos pela CONTRATANTE.

3.3.3 Sistema disponível em regime 24X7 (vinte e quatro horas por dia, sete dias por semana em qualquer período do ano).

3.3.4 O suporte deverá ser todo no idioma local, ou seja, português do Brasil.

3.3.5 Demais requisitos serão pormenorizados no Termo de Referência.

3.4 Requisitos Regulatórios

3.4.1 Compliance: Conformidade com LGPD, ISO 27001, NIST Cybersecurity Framework;

3.4.2 Auditoria: Logs detalhados, com telemetria completa e suporta a auditoria e análise forense;

3.4.3 Relatórios: Geração automática de *dashboards* de risco (executivo) e relatórios de conformidade regulatória;

3.4.4 Demais requisitos serão pormenorizados no Termo de Referência.

3.5 Requisitos de Treinamento

3.5.1 A CONTRATADA deverá realizar treinamento sobre a utilização da solução de antivírus fornecida. O treinamento deve envolver toda a estrutura da solução e seus módulos. Após o treinamento, a equipe técnica da CONTRATANTE deverá estar apta a efetuar a instalação, configuração, atualização e gerenciamento da solução.

3.5.1.1 O treinamento deverá envolver aspectos teóricos e aspectos práticos.

3.5.1.2 A carga horária mínima do treinamento deverá ser de 8 (oito) horas.

3.5.2 Demais requisitos serão pormenorizados no Termo de Referência.

3.6 Níveis mínimos de serviço

3.6.1 Para a execução da presente contratação será utilizado como critério de aferição os resultados dos Níveis Mínimos de Serviço (SLA).

3.6.1.1 Os níveis mínimos de serviços se constituem em critérios objetivos e mensuráveis estabelecidos entre a CONTRATADA e o CONTRATANTE com a finalidade de aferir e avaliar a prestação dos serviços contratados.

3.6.1.2 Para mensurar esses fatores são utilizados indicadores relacionados com a natureza e características dos serviços a serem contratados, os quais serão estabelecidas metas quantificáveis a serem cumpridas pela CONTRATADA.

3.6.2 A CONTRATADA será responsável pelo cumprimento, medição e envio das informações dos indicadores estabelecidos durante todo o prazo de vigência do contrato.

3.6.2.1 A medição dos indicadores estabelecidos serão auditados pela CONTRATANTE durante todo o prazo de vigência do contrato.

3.6.2.2 Os indicadores poderão ser revistos, a qualquer tempo, com vistas à melhoria ou ajustes na qualidade dos serviços prestados, desde que acordado entre as partes.

3.6 3 SLA: Tempo resposta máximo de 4h para incidentes classificados como Prioridade 1 (P1).

3.6 4 Deverão ser atendidas demais especificações para os níveis mínimos de serviço estabelecidos no Termo de Referência.

3.7 Comprovação de experiência prévia quanto ao objeto da contratação

3.7.2 A CONTRATADA deverá apresentar atestados de capacidade técnica, emitidos por pessoa jurídica de direito público ou privado, que comprovem a prestação de serviços de natureza e complexidade técnica similares às exigidas na contratação, com a comprovação de fornecimento de no mínimo 5.000 (cinco mil) licenças/ano;

3.7.2.1 Será aceito o somatório de atestados e/ou declarações para comprovar a capacidade técnica.

3.7.2.2 A exigência de comprovação de fornecimento na quantidade estipulada no item 3.7.2 justifica-se pela necessidade de fornecimento de licenças e gerenciamento em larga escala do ambiente da Contratante.

3.7.4 Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora;

3.7.5 Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou filial da licitante;

3.7.6 Não serão aceitos atestados emitidos pela licitante, em seu próprio nome, nem qualquer outro em desacordo com as exigências do Edital;

3.7.7 A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

3.8 Prazos de execução e de vigência da contratação

3.8.1 O prazo de execução será de 60 (sessenta) meses, a contar da emissão da Ordem de Serviço, prorrogável na forma do Art. 107 da Lei nº 14.133/2021, vez que a contratação está prevista no Plano Plurianual.

3.8.2 O prazo de vigência contratual será de 62 (sessenta e dois) meses, a contar da data de assinatura do respectivo contrato, vez que a contratação está prevista no Plano Plurianual, podendo ser prorrogado na forma do Art. 107 da Lei nº 14.133/2021, conforme as necessidades e conveniência da Administração Pública Municipal.

3.8.3 As definições de prazo têm por fundamento a natureza do serviço a ser contratado, que se enquadra na categoria de serviço contínuo, conforme o artigo 6º, inciso XV, da Lei n.º 14.133/2021.

3.9 Garantia contratual nos termos do Art. 96 da Lei 14.133/2021.

3.9.1 Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021,

em seu inciso XII, no percentual de 2% (dois por cento) e condições descritas nas cláusulas do contrato.

3.9.2 Demais requisitos serão pormenorizados no Termo de Referência.

3.10 Dos requisitos de proteção de dados pessoais

3.10.1 A solução deverá observar e cumprir rigorosamente todos os dispositivos legais previstos na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), na Lei nº 12.965/2014 (Marco Civil da Internet) e demais normas aplicáveis à proteção de dados pessoais e segurança da informação.

3.10.2 Demais requisitos serão pormenorizados no Termo de Referência.

Por fim, para a adequada satisfação da necessidade da Administração devem ser atendidos os requisitos acima dispostos, bem como demais requisitos específicos dispostos no Termo de Referência e Anexo I - Especificações Técnicas.

4 – ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO (obrigatório)

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, este campo é obrigatório.

4.1 A contratação tem como quantitativo estimado as licenças adquiridas atualmente (9.000/ano) conforme o Termo de Contrato Nº 369/2024 - (SEI 0020173638), com acréscimo de licenças, a fim de atender às seguintes necessidades:

4.1.1 O contrato atual visa proteger apenas as estações de trabalho, sendo necessário estender essa proteção também para as demais fontes de acesso à rede como: dispositivos móveis (aparelhos de celular corporativos), tablets, notebooks e equipamentos;

4.1.2 Aumento de dispositivos a serem protegidos em decorrência do ingresso de novos servidores públicos pelo Concurso Público (Edital Nº 001/2024/SGP.UDS);

4.1.3 O contrato atual tem como prazo de execução o período de 12 (doze meses), no entanto, por tratar-se de serviço contínuo e visando a eficiência administrativa, se faz necessário que a nova contratação seja prolongada para o período de 60 (sessenta meses), correspondente a 5 (cinco) anos;

4.1.4 Aumento da carga horária dos servidores lotados no cargo de Agente Administrativo e Analista de Tecnologia da Informação, em conformidade com as Leis Complementares Nº 728, de 01 de outubro de 2025 e nº 714/2025, de 07 de agosto de 2025, o que implica no fim de revezamento de períodos de postos de trabalho em muitos setores, resultando no aumento da quantidade de computadores.

4.2 Diante do exposto, a quantidade estimada preliminar é de:

Item	Especificação	Unidade	Quantidade Ano 1	Quantidade Ano 2	Quantidade Ano 3	Quantidade Ano 4	Quantidade Ano 5
1	Solução corporativa de antivírus e antimalware com tecnologia EDR (aquisição temporária de licenças, atualizações, manutenção e suporte técnico para estações de trabalho, dispositivos móveis e servidores)	Serviço (Licenças de Uso de Software)	20.000	20.000	20.000	20.000	20.000

4.2.1 Os quantitativos apresentados na tabela do item 4.2, se referem ao **quantitativo máximo anua**l que poderá ser contratado, sendo que o quantitativo mínimo anual será de 10.000 (dez mil) licenças.

5 - LEVANTAMENTO DE MERCADO

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, em caso do não preenchimento deste campo, devem ser apresentadas as devidas justificativas.

De acordo com a pesquisa de mercado realizada, foi possível elencar as seguintes soluções:

Solução A: Plataforma EPP (Foco em Prevenção Básica/Avançada, como Anti-Malware, Firewall de *Host* e Controle de Aplicações).

O objetivo central de uma plataforma EPP é bloquear a maioria das ameaças antes que elas causem qualquer dano, agindo como um escudo para o endpoint. Em essência, a plataforma EPP é a fundação da sua estratégia de cibersegurança, garantindo que a maioria dos perigos seja detida antes da invasão. No entanto, para as

ameaças mais persistentes e sofisticadas que conseguem contornar essa prevenção, se faz necessário o EDR, fornecendo as capacidades de detecção, visibilidade e resposta.

Solução B: Plataforma EDR (Foco em Prevenção Next-Gen (NGAV) e Resposta Rápida e Threat Hunting no Endpoint).

A Plataforma EDR consiste em uma solução *Endpoint Detection and Response*, ou seja, uma solução de Detecção e Resposta de Ponto de Acesso ou Ponto de Extremidade. É uma tecnologia de cibersegurança avançada, focada em proteger os endpoints de uma organização. Endpoints são os diversos dispositivos conectados (computadores, notebooks, equipamentos servidores, entre outros). Diferente de antivírus tradicionais, que focam em prevenção baseada em assinaturas de ameaças conhecidas, o EDR adota uma abordagem proativa e contínua. O objetivo é garantir que seu dispositivo (o endpoint) esteja protegido antes, durante e depois de um ataque. Ainda, este recurso permite que a organização restrinja o que pode ser executado e conectado aos endpoints, reduzindo a superfície de ataque. Essa é a solução que melhor atende à necessidade da Administração, à medida que a plataforma oferece uma estratégia de segurança em duas etapas: a primeira, o bloqueio em massa e, a segunda, detecção e erradicação, garantindo que nada passe despercebido. Essa abordagem holística é o padrão ouro da segurança de endpoints na atualidade.

Solução C: Plataforma XDR (Foco em Visibilidade e Resposta Unificadas e Abrangentes em Todo o Ecossistema de TI).

A Plataforma XDR (Extended Detection and Response - Detecção e Resposta Estendidas) é a evolução natural do EDR e representa o futuro da cibersegurança empresarial. A Plataforma XDR correlaciona dados e, por esse motivo, transforma dados desconexos em inteligência acionável, permitindo que as equipes de segurança reajam a ataques complexos e multifacetados com velocidade. No entanto, o uso de uma plataforma XDR, além de representar alto custo, exige uma alta capacidade de processamento de dados e traz maior consumo de banda nos links de dados, o que comprometeria a usabilidade dos dispositivos e poderia sobrecarregar a rede atual. Considerando que atualmente na Prefeitura Municipal de Joinville grande parte do parque tecnológico consiste em Windows 10, o uso de uma solução que requer alta capacidade de processamento de dados implicaria na sobrecarga de processamento local das estações, interrupção dos trabalhos e impacto direto na prestação de serviços.

A partir das soluções apresentadas, tem-se o seguinte diagnóstico:

Solução (Tipo)	Requisitos Técnicos Funcionais:	Requisitos de Performance:	Requisitos de Suporte	Requisito 4 (Detecção Avançada/Hunting)	Requisito 5 (Visibilidade Abrangente)
Solução A (EPP)	Prevenção Básica	Leve/Foco no Antivírus	**não atende**	**não atende**	**não atende**
Solução B (EDR)	Prevenção e Resposta no Endpoint	Plataforma otimizada	Suporte 24/7	Detecção e Resposta no Endpoint	Boa visibilidade no Endpoint
Solução C (XDR)	Visão de Segurança Completa	**não atende**	Suporte 24/7	Hunting em Multi-Domínio	Máxima visibilidade em toda a superfície

CONCLUSÃO - MELHOR SOLUÇÃO

Considerando as soluções supra elencadas, os requisitos da Administração em relação à capacidades técnicas, relação custo-benefício e adequação ao ambiente público, além da vasta concorrência identificada e a necessidade de incorporar tecnologias avançadas, como o EDR, demonstra-se que a contratação de empresa especializada na prestação de serviços de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint), conforme especificações técnicas, com disponibilização de atualizações, manutenção e suporte técnico é a melhor solução para atendimento ao interesse público.

6. ESTIMATIVA DO VALOR DA CONTRATAÇÃO (obrigatório)

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, este campo é obrigatório.

Considerando o montante estimado para o objeto conforme o Item 4 do presente Estudo Técnico Preliminar (ETP), que totaliza 100.000 (cem mil) licenças distribuídas ao longo de 60 (sessenta) meses (sendo 20.000 licenças/ano), e, tendo como base os valores de contratações similares e pesquisa com fornecedores, demonstrados no documento "orçamentos planilhados SEI 27195529", estima-se que o valor global da contratação seja de **R$ 21.000.000,00 (vinte e um milhões de reais),** cujo montante deverá ser devidamente ajustado à real necessidade, quando da finalização dos estudos.

7 - DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, em caso do não preenchimento deste campo, devem ser apresentadas as devidas justificativas.

A presente contratação tem como objetivo obter serviços especializados de solução de segurança cibernética, abrangendo antivírus e antimalware com tecnologia de Detecção e Resposta de Endpoint (EDR), conforme especificações técnicas estabelecidas, incluindo a disponibilização de atualizações, manutenção e suporte técnico.

Busca-se assegurar a proteção avançada e contínua dos ativos computacionais da Prefeitura Municipal de Joinville, por meio da prevenção, detecção, análise e resposta a ameaças cibernéticas, garantindo maior eficiência no tratamento de incidentes de segurança.

A adoção de solução com tecnologia EDR permitirá o monitoramento em tempo real dos endpoints, a identificação de comportamentos anômalos, a mitigação de vulnerabilidades e a rápida contenção de ataques, reduzindo riscos operacionais e contribuintes para a integridade, disponibilidade e confidencialidade das informações.

Além disso, a contratação visa assegurar a atualização permanente das ferramentas de proteção, bem como o acesso a suporte técnico especializado durante toda a vigência do contrato, garantindo o pleno funcionamento da solução e o alinhamento às melhores práticas de segurança da informação.

Assim, após análise das soluções de mercado, verifica-se que a contratação de empresa especializada na prestação de serviços de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint), conforme especificações técnicas, com disponibilização de atualizações, manutenção e suporte técnico é a melhor solução para atendimento ao interesse público.

8. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO (obrigatório)

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, este campo é obrigatório.

A solução de segurança cibernética constitui sistema integrado indivisível pelas seguintes razões técnicas:

Interdependência Técnica

- Console único necessário para visibilidade unificada de ameaças;
- Base de dados correlacionada de eventos de segurança;
- Políticas de segurança centralizadas e consistentes;
- *Threa*t *intelligence* compartilhada entre todos os *endpoints*.

Eficiência Operacional

- Gerenciamento único reduz complexidade administrativa;
- Treinamento unificado da equipe técnica;
- SLA homogêneo para toda infraestrutura;
- Economia de escala na contratação.

Requisitos de Segurança

- Necessidade de visão holística das ameaças;
- Correlação de eventos entre diferentes dispositivos;
- Resposta coordenada a incidentes de segurança;
- Padronização de políticas de proteção;
- O parcelamento comprometeria a eficácia da proteção e aumentaria custos operacionais sem benefícios técnicos ou econômicos.

A presente solução não é divisível, considerando a natureza do serviço a ser contratado, tratando-se da contratação de empresa especializada na prestação de serviços de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint), conforme especificações técnicas, com disponibilização de atualizações, manutenção e suporte técnico, solução esta cuja administração demanda suporte e licenciamento unificados para o correto funcionamento.

9 - DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, em caso do não preenchimento deste campo, devem ser apresentadas as devidas justificativas.

O resultado pretendido da presente contratação é a proteção e a segurança das informações pertencentes à Administração Pública Municipal. A disponibilização de solução corporativa de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint), permite à Prefeitura de Joinville evitar a contaminação de redes por vírus, *spywares, malwares, adwares, phishing, rootkits*, cavalos de tróia, *worms, keyloggers, netbot*s e outros tipos de códigos maliciosos que os equipamentos de informáticas estão sujeitos.

Destacamos também que a contratação desse tipo de solução corporativa é uma das ações possíveis para a

promoção de cibersegurança, sendo essencial para impulsionar a implantação de novas tecnologias, garantindo a segurança no desenvolvimento de ações que promovam a transformação digital, contribuindo para o desenvolvimento econômico e social do município e, considerando que a modernização da Administração Pública é componente essencial para a estratégia de desenvolvimento da cidade, investir em transformação digital no serviço público traz uma série de vantagens e é cada vez mais reconhecido como uma necessidade para uma Administração eficiente.

10. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, em caso do não preenchimento deste campo, devem ser apresentadas as devidas justificativas.

10.1 Não há a necessidade de contratações prévias e também não serão necessárias providências adicionais, visto que a contratação do objeto definido é de maneira completa, evitando a necessidade de investimentos em treinamento, aquisição de equipamentos e contratações individuais de servidores.

10.2 Importante pontuar que, quanto à equipe técnica de fiscalização, essa Secretaria possui servidores com experiência técnica e conhecimento acerca do produto a ser adquirido, bem como, caso necessário, pode-se solicitar o suporte das demais Secretarias.

10.3 Ainda, cumpre ressaltar que, quando da indicação dos membros para fiscalização do contrato, em atendimento ao princípio da segregação de funções, o ordenador da despesa deverá observar que não se recomenda que os membros da elaboração da fase preparatória atuem como membros da comissão de fiscalização.

11. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, em caso do não preenchimento deste campo, devem ser apresentadas as devidas justificativas.

Não há contratações correlatas e/ou interdependentes, pois compete à Diretoria de Tecnologia e Gestão da Secretaria de Administração e Planejamento a contratação de forma unificada e centralizada de equipamentos de Tecnologia da Informação e Comunicações (TIC) para atendimento das necessidades dos demais órgãos da Administração, inclusive com vistas ao atendimento dos princípios da eficiência, planejamento e centralização das compras.

Outrossim, para a presente contratação, não há interesse da Administração em aderir às Atas de Registros de Preços dos Consórcios, pelos seguintes motivos sucintamente elencados:

1) Complexidade na gestão: A participação em um consórcio exige uma gestão eficiente e coordenada entre os membros participantes. Isso pode apresentar desafios adicionais, pois envolve a coordenação de interesses, tomada de decisões conjuntas e resolução de conflitos, principalmente em se tratando de compras unificadas, que atendem aos diversos órgãos da Administração. A falta de uma gestão adequada pode levar a atrasos e problemas operacionais.
2) Menor flexibilidade: Participar de um consórcio pode exigir que os órgãos públicos sigam determinadas regras, regulamentos e procedimentos estabelecidos pelo Consórcio. Isso pode resultar em uma menor flexibilidade na condução das licitações, impedindo que os órgãos públicos adotem abordagens mais personalizadas ou específicas para suas necessidades individuais, bem como conflitar com a prática administrativa. Por exemplo, no caso do CINCATARINA, conforme sua Resolução 104/2024, o Estudo Técnico é dispensado para determinados grupos. Compulsando o rol de objetos "dispensados" constata-se que estes se enquadram na quase totalidade dos objetos licitados por meio das compras unificadas. No entanto, como visto, a dispensa da elaboração do Estudo Técnico Preliminar pelo Consórcio não desobriga a Administração da elaboração do mesmo (Art. 9º), causando evidente contrassenso, vez que, na hipótese de indicar o quantitativo (IRP), salvo melhor juízo, não sabe se o Consórcio elaborou ou não o ETP, e ao aderir, salvo melhor juízo, estará elaborando um este ETP após o processo licitatório.
3) Complexidade na gestão de contratos: A gestão de contratos pode se tornar mais complexa em um Consórcio, especialmente quando há a participação de vários membros. Coordenar as obrigações contratuais, as responsabilidades e as expectativas de todos os membros requer uma gestão eficiente e uma comunicação clara, principalmente em se tratando de compras unificadas, que atendem aos diversos órgãos da Administração.
4) Restrições de autonomia: Participar de um consórcio pode implicar em restrições à autonomia dos órgãos públicos. Isso ocorre porque as decisões sobre as licitações podem precisar ser tomadas de forma conjunta, considerando os interesses e necessidades de todos os membros, bem como devem estar alinhadas às decisões tomadas pelo Consórcio, enquanto gestor da ARP.
5) Possíveis atrasos: Devido à natureza colaborativa dos consórcios, pode haver atrasos no processo de tomada de decisão. A necessidade de consulta e consenso entre os membros pode prolongar o tempo necessário para finalizar as etapas do processo licitatório. Isso pode ser problemático em situações em que é exigida uma resposta rápida ou quando há prazos rígidos. Ademais, na condição de Consorciado e participante, o órgão aderente não detém qualquer ingerência nas decisões tomadas pelo Consórcio no decorrer da gestão e execução contratual.
6) Necessidade de garantir a transparência e o controle do processo de contratação pública. Ao realizar

contratações independentes, o Município tem maior controle sobre o processo como um todo, desde seu início até sua conclusão, podendo adotar medidas adicionais para assegurar a lisura e a transparência em todas as etapas. Isso inclui a elaboração de editais de licitação, a realização de julgamentos e a publicidade adequada dos resultados, fortalecendo a credibilidade e a confiança na Administração Municipal.

7) As contratações através dos Consórcios podem englobar uma ampla gama de fornecedores e produtos, nem sempre passando por rigorosos processos de seleção e avaliação conforme é realizado pela Administração. Assim, ao realizar contratações independentes (próprias), o Município pode estabelecer critérios de seleção necessários ao atendimento da demanda, buscando garantir a qualidade e segurança dos produtos e serviços contratados, bem como a idoneidade das empresas envolvidas.

Para análise do interesse público, a Administração deve acima de tudo buscar a eficiência em suas contratações. Na tomada de decisão acerca da viabilidade e interesse público em participar ou aderir a uma Ata de Registro de Preços dos Consórcios é necessário avaliar vários fatores que não somente preços, mas se as condições propostas para contratação são realmente vantajosas para o Município, ou mesmo o completo atendimento pelo Consórcio do que determina à Lei para as fases preparatória, licitatória e executiva.

Assim, não havendo a manifestação de Interesse de Registro de Preços - IRP ou Manifestação de Órgão Participante - MOP nos Consórcios aos quais o Município de Joinville integra, resta evidente, diante dos pontos ora elencados, que não há interesse da Administração em utilizar dos referidos processos licitatórios dos Consórcios para fins de contratação do objeto ora licitado.

Por fim, ressalta-se que a Administração possui capacidade tanto de pessoal como técnica para realizar a contratação do objeto em questão.

12. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, em caso do não preenchimento deste campo, devem ser apresentadas as devidas justificativas.

Impactos Positivos

- Redução de infraestrutura física local (solução cloud);
- Diminuição do consumo energético de servidores locais;
- Redução de deslocamentos por gerenciamento remoto.

Impactos Neutros/Mínimos

- Aumento marginal no tráfego de dados (cloud);
- Eventual descarte de equipamentos obsoletos.

Medidas Mitigadoras

- Descarte Responsável: Contratada deve seguir logística reversa para equipamentos, quando aplicável;
- Eficiência Energética: Priorização de datacenters verdes do fornecedor;
- Otimização de Recursos: Configuração otimizada para reduzir tráfego desnecessário.

Conclusão

A prestação de serviços de antivírus, antimalware e EDR apresenta baixos impactos ambientais diretos, sendo a maioria de natureza indireta e associada ao uso de infraestrutura tecnológica. As medidas mitigadoras propostas asseguram que a contratação esteja alinhada às boas práticas de sustentabilidade, responsabilidade socioambiental e uso racional de recursos.

13. ANÁLISE DE RISCOS

De acordo com o art. Art. 18, inciso X da Lei 14.133/2021, na fase preparatória, devem ser abordados os riscos que possam comprometer o sucesso da licitação e a boa execução contratual

13.1 Analisando os riscos da contratação, podemos indicar os seguintes elementos:

13.1.1 Identificação de Riscos: dentre os riscos analisados e expostos no Mapa/Matriz de Riscos SAP.UNG (SEI nº 27059778) da presente contratação, destacamos que o risco de grau mais elevado está concentrado na capacidade do fornecedor honrar seus compromissos contratuais, especialmente em relação ao fornecimento de materiais de reposição/manutenção durante a vigência do contrato, considerando o cenário econômico internacional, especialmente questões tarifárias de importação que impõem ônus demasiados aos fornecedores nacionais.

13.1.2 Análise de Riscos: considerando a identificação do risco no ponto 13.1.1 do presente documento, recai sobre a presente contratação o risco de o contrato sobre alterações de cunho econômico que ultrapassem os limites legais, levando ao estado de sobrepreço, nos termos do Art. 6, inciso LVI da Lei Federal n.º 14.133, impossibilitando, portanto, o reequilíbrio contratual por parte da Administração Pública.

13.1.3 Avaliação de riscos: dos riscos encontrados, procedendo à ponderação do impacto e da probabilidade, constatamos que os riscos relativos à seleção do fornecedor são classificados como "Alto".

13.1.4 Tratamento de riscos: com base na análise realizada, esta equipe de planejamento entende que se deve adotar as seguintes condutas:

13.1.4.1 Manter uma equipe multidisciplinar dedicada para o acompanhamento e fiscalização do contrato, requerendo da Contratada, sempre que solicitada, mas especialmente durante a fase de habilitação, que apresente instrumentos formais que atestem parcerias com empresas de fornecimento de materiais de gestão de infraestrutura de Tecnologia de Informação e peças para manutenção preventiva e corretiva de países europeus, asiáticos ou de outros países latino-americanos não afetados pelas tarifas americanas e/ou outros meios de prova de reorganização logística, como nacionalização da cadeia de suprimentos ou triangulação comercial, p. ex., de modo a proporcionar o reequilíbrio contratual dentro dos limites legais;

13.1.4.2 Formalizar as tomadas de decisões;

13.1.4.3 Cobrar ativamente a regularidade fiscal e notificar a empresa na ausência das documentações;

13.1.4.4 Realizar acompanhamento do prazo de entrega, avaliando as causas de possíveis atrasos, para tratá-las;

13.1.4.5 Aplicar notificação, providência de sanções administrativas sem prejuízo, além de outras providências necessárias para a correta execução contratual e responsabilização da empresa, quando necessário;

13.1.4.6 Realizar os estudos técnicos preliminares como pré-requisito para a elaboração do termo de referência e seus anexos, buscando ainda a padronização das especificações, de modo a tornar factível a operacionalização do contrato;

13.1.4.7 Promover pesquisas de satisfação junto aos usuários (feedback) durante períodos semestrais e/ou trimestrais, a fim de averiguar a satisfação com a prestação de serviço.

Essas medidas mitigadoras foram pensadas para diminuir as chances de ocorrerem riscos e também para minimizar seus possíveis impactos. Assim, elas ajudam a garantir que a licitação seja bem-sucedida e a execução do contrato, que envolve o serviço de suporte técnico e a gestão de ativos, aconteça de forma eficiente, trazendo os benefícios esperados para o Município.

14. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA (obrigatório)

De acordo com o art. Art. 18, §º 2º da Lei 14.133/2021, este campo é obrigatório.

14.1 Para proceder à análise da viabilidade da contratação, esta deve atender positivamente os seguintes critérios:

Parâmetro considerado	Sim	Não	Observação / Comentário
1. O modelo adotado para a contratação é o mais vantajoso para a Administração, tanto pelo aspecto técnico como pelo econômico?	x		
2. O modelo adotado para a contratação está em conformidade com o praticado no mercado?	x		
3. O valor estimado da contratação está em conformidade com a previsão orçamentária?	x		
4. Os resultados pretendidos com a contratação compensam os investimentos realizados pela Administração, em curto, médio e longo prazo?	x		
5. De acordo com a análise dos riscos para a contratação, a contratação é viável e não possui risco de dano ao erário? (moderado/médio a grave)	x		

6. Há risco de comprometimento do sucesso da licitação e da execução, considerando os fatos ocorridos em contratações anteriores do mesmo objeto ou similares.		x	
7. No caso do item anterior, foram indicadas as medidas necessárias para mitigar os riscos?			Não se aplica.

CONCLUSÃO:

Com base neste Estudo Técnico Preliminar, a Equipe/Comissão de Planejamento declara viável a contratação de empresa especializada na prestação de serviços de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint), conforme especificações técnicas, com disponibilização de atualizações, manutenção e suporte técnico pelo período de 60 (sessenta) meses, nos moldes descritos no presente Estudo Técnico Preliminar, vez que se mostrou a solução técnica e economicamente mais adequada à necessidade da Administração e fundamentadamente atende ao interesse público.

Documento assinado eletronicamente por **Anna Paula Pinheiro**, **Diretor (a) Executivo (a)**, em 03/12/2025, às 09:49, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

Documento assinado eletronicamente por **Rodrigo Ponick**, **Gerente**, em 03/12/2025, às 09:55, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

Documento assinado eletronicamente por **Grasiele Wandersee Philippe**, **Coordenador(a)**, em 03/12/2025, às 09:57, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

Documento assinado eletronicamente por **Alessandro de Cassio Silva**, **Servidor(a) Público(a)**, em 03/12/2025, às 10:06, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

A autenticidade do documento pode ser conferida no site https://portalsei.joinville.sc.gov.br/ informando o código verificador **27711447** e o código CRC **F2AF3D69**.