JULGAMENTO DA IMPUGNAÇÃO SEI Nº 28625994/2026 - SAP.LCT

Joinville, 03 de março de 2026.

FEITO: IMPUGNAÇÃO ADMINISTRATIVA

REFERÊNCIA: EDITAL PREGÃO ELETRÔNICO Nº 092/2026

OBJETO: CONTRATAÇÃO DE ANTIVÍRUS E ANTIMALWARE COM TECNOLOGIA EDR (DETECÇÃO E RESPOSTA DE ENDPOINT)

IMPUGNANTE: NP SOLUÇÕES EM TI LTDA

I – DAS PRELIMINARES

Trata-se de Impugnação Administrativa interposta pela empresa **NP SOLUÇÕES EM TI LTDA** contra os termos do Edital de Pregão Eletrônico nº 092/2026, do tipo menor preço global, destinado à Contratação de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint).

II – DA TEMPESTIVIDADE

No tocante à tempestividade, verifica-se a regularidade da presente impugnação, recebida na data de 26 de fevereiro de 2026, atendendo ao preconizado no art. 164 da Lei nº 14.133/21, bem como o disposto no subitem 11.1 do edital.

No tocante à representatividade, a empresa atende ao disposto no subitem 11.1.1 do edital.

Deste modo, passamos a analisar o mérito da presente impugnação.

III – DAS ALEGAÇÕES DA IMPUGNANTE

A empresa NP Soluções em TI Ltda apresentou impugnação ao Edital pelas razões abaixo descritas.

Em síntese, a Impugnante alega que o Edital, ao exigir funcionalidades de firewall (NGFW), webfilter e reputação de URL, gerenciamento de dispositivos móveis (MDM) e criptografia de discos, extrapola o escopo de uma solução EDR.

Prossegue argumentando que tais exigências, somadas à obrigatoriedade de console On-Premise e criação de assinaturas HIPS, vacinas personalizadas, restringem a competitividade.

Ao final, requer o recebimento e o provimento da presente Impugnação, com a consequente retificação do Edital.

IV – DO MÉRITO

Inicialmente, importa considerar que todos os procedimentos licitatórios processados em âmbito nacional devem estar estritamente pautados na legislação e nos princípios que norteiam o processo formal de aquisição e contratação governamental.

Deste modo, cabe ressaltar que a Administração procura sempre o fim público, respeitando

todos os princípios basilares da licitação e dos atos administrativos, sobretudo o princípio da legalidade, da isonomia, da vinculação ao Instrumento Convocatório e o julgamento objetivo. Tais princípios norteiam essa atividade administrativa, impossibilitando o Administrador de fazer prevalecer sua vontade pessoal, e impõem ao mesmo o dever de pautar sua conduta segundo as prescrições legais e editalícias.

Aliás, este é o ensinamento da Lei nº 14.133/21, que prescreve, *in verbis*:

> Art. 5º Na aplicação desta Lei, serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da probidade administrativa, da igualdade, do planejamento, da transparência, da eficácia, da segregação de funções, da motivação, da vinculação ao edital, do julgamento objetivo, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável, assim como as disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

Assim, considerando que os pontos impugnados decorrem da fase de planejamento do processo licitatório, a presente impugnação foi encaminhada para análise e manifestação da Unidade de Governança e Contratações de TIC, da Secretaria de Administração e Planejamento, unidade responsável pelo planejamento do presente processo.

Em resposta, a Unidade de Governança e Contratações de TIC se manifestou através do Memorando SEI Nº 28625465/2026 - SAP.UGC, o qual transcrevemos:

> Cumprimentando-os cordialmente, em atenção ao memorando em epígrafe, servimo-nos do presente para encaminhar a análise técnica da Impugnação ao Edital 1 , documento SEI n° 28584200, interposto pela empresa **NP SOLUÇÕES EM TI LTDA**.
>
> Em síntese, a impugnante alega que as especificações técnicas extrapolam o escopo de uma solução EDR, abrangendo funcionalidades de *Firewall* (NGFW), MDM, Criptografia e Filtro Web.
>
> Argumenta que tais exigências, somadas à obrigatoriedade de console *On-Premise* e criação de assinaturas HIPS, restringem a competitividade e ferem a Lei nº 14.133/2021.
>
> Requer, portanto, a segregação das exigências e a republicação do edital.
>
> Após análise técnica dessa Unidade, as alegações não procedem pelos seguintes motivos:
>
> **1. Do Escopo do Objeto e a Discricionariedade Técnica**
>
> A alegação de que as exigências extrapolariam o escopo do item 1.1.1 ("Antivírus e Anti-malware com EDR") revela uma visão reducionista do certame. A nomenclatura inicial é uma definição simplificada para fins de classificação orçamentária, mas o objeto de uma licitação é definido pelo **conjunto indissociável** de especificações dos seus Anexos Técnicos.
>
> Conforme o **Art. 18, I, da Lei nº 14.133/2021**, a fase preparatória é balizada pela "descrição da necessidade da administração". No cenário atual de ameaças, as soluções de segurança de *endpoint* evoluíram de simples antivírus para plataformas integradas (**EPP/EDR/XDR**). Funções como firewall de host, MDM e criptografia não são "adicionais", mas especificações qualificadas que garantem a **eficiência administrativa**, evitando a fragmentação da segurança em múltiplos softwares e contratos distintos.
>
> **2. Da Natureza do Objeto e a Não Confusão com NGFW (Itens 4.1.69 a 4.1.72)**
>
> Não prospera a tese de que controles de TCP/UDP, DNS e proteção contra DoS sejam exclusivos de soluções de borda (*Next-Generation Firewall*).
>
> **- Diferenciação Técnica:** As funcionalidades exigidas nos itens 4.1.69 a 4.1.72 referem-se ao Host-Based Firewall. Diferente do NGFW, que atua no perímetro da rede, o firewall de host é intrínseco às plataformas modernas de EDR/EPP.
>
> **- Finalidade:** Tais controles são essenciais para identificar e bloquear a movimentação lateral de atacantes dentro da rede interna, onde o firewall de borda não possui visibilidade. Trata-se de uma camada de defesa em profundidade necessária para a proteção do ativo público.
>
> **- Trabalho Remoto:** Com o aumento do uso de notebooks fora da rede da

Prefeitura, o endpoint torna-se seu próprio perímetro. Sem as funcionalidades de firewall pessoal exigidas, o dispositivo estaria vulnerável ao se conectar em redes públicas, de outras instituições ou domésticas.

3. Do Webfilter e Reputação de URLs (Itens 4.1.68 e 4.1.105)

Embora o impugnante alegue que estas são funções de *Secure Web Gateway* , elas são componentes fundamentais de prevenção em soluções de *endpoint* modernas.

O *Webfilter* no endpoint é a primeira linha de defesa contra o *phishing* e o acesso a domínios maliciosos. Exigir que o EDR possua essa capacidade visa impedir que a ameaça sequer seja baixada para o host, otimizando a segurança antes mesmo da necessidade de detecção por comportamento.

Atualmente, quase todo o tráfego da web é criptografado (SSL/TLS). Um Firewall de borda, para enxergar o que há dentro desse tráfego, precisa realizar uma técnica custosa e que não funciona 100% das vezes, chamada de "SSL Inspection". O Webfilter no Endpoint atua "dentro" do sistema operacional, no ponto exato onde os dados são processados antes de serem criptografados pelo navegador. Isso permite que a solução identifique uma URL maliciosa que passaria "disfarçada" por um túnel criptografado no firewall de rede.

4. Do Gerenciamento de Dispositivos Móveis – MDM (Itens 3.1.44 e 3.1.45)

A alegação do impugnante de que a gestão de dispositivos móveis Android e iOS caracteriza uma "solução distinta" (MDM/UEM) e não integra o escopo de um EDR é improcedente, conforme os seguintes fundamentos:

- A inclusão de Android e iOS no escopo é imperativa e fundamentada no **Princípio da Economicidade (Art. 5º, Lei 14.133/21)**.

- Convergência para o Modelo EPP/UEM: O mercado de cibersegurança consolidou o conceito de Endpoint Protection Platform (EPP), onde o "endpoint" (ponto de extremidade) não se restringe mais ao desktop. Dispositivos móveis são, hoje, vetores críticos de entrada em redes corporativas. Fabricantes líderes de mercado (líderes no Gartner e Forrester, conforme exigido no item 1.3 do Anexo I) integram nativamente o gerenciamento de ameaças móveis em suas consoles de EDR para garantir a visibilidade total do perímetro.

- Fundamentação Legal – Eficiência e Economicidade (Art. 5º, Lei 14.133/21): A Administração Pública tem o dever de buscar a eficiência. Exigir que a solução de segurança suporte dispositivos móveis sob a mesma console e agente evita a fragmentação da gestão. A contratação separada de um MDM exigiria novos custos de licitação, integração de APIs, treinamento de pessoal e dupla infraestrutura, o que feriria o Princípio da Economicidade e o interesse público.

- Justificativa Técnica do QR Code e Provisionamento (Item 3.1.45): A exigência de instalação via QR Code, link ou e-mail não é uma restrição, mas um requisito de agilidade operacional. Em uma estrutura pública com centenas de dispositivos, o provisionamento simplificado é essencial para garantir que o parque tecnológico seja protegido rapidamente. Tais métodos de implantação são recursos padrão nas versões corporativas das suítes de EDR/EPP de mercado.

- Unificação de Políticas de Segurança: A integração do MDM ao ecossistema de segurança do endpoint permite que uma única política de conformidade seja aplicada. Caso um dispositivo móvel seja comprometido ou perdido, a console de EDR centralizada pode executar ações de resposta (como o *remote wipe* ou isolamento), garantindo que o celular corporativo não se torne uma "ponte" para ataques à rede interna da Prefeitura.

- Interoperabilidade e LGPD: Em conformidade com a LGPD, a Administração deve assegurar a proteção dos dados em trânsito. Dispositivos móveis que acessam e-mails e sistemas governamentais devem estar sob o mesmo rigor de monitoramento de ameaças que os computadores locais, justificando a exigência técnica contida nos anexos.

5. Da Criptografia de Discos (Item 4.2)

A impugnação afirma que a criptografia de discos é uma solução autônoma e não obrigatória em EDRs.

A gestão centralizada da criptografia é uma medida de segurança física e lógica. Em cumprimento à LGPD, o Município deve assegurar que o extravio de um notebook não resulte em vazamento de dados sigilosos. A exigência apenas reflete o padrão de alta performance do mercado atual; a

incapacidade de um licitante em ofertar a função não deve compelir a Administração a reduzir seu nível de proteção.

A Lei Geral de Proteção de Dados (LGPD) impõe ao ente público o dever de salvaguardar dados sensíveis. A gestão centralizada da criptografia pelo agente de segurança do endpoint garante que, em caso de perda ou furto do equipamento físico, os dados do município permaneçam protegidos, unindo a segurança lógica à física.

A ausência de uma gestão de criptografia centralizada pode ser interpretada como negligência em caso de vazamento de dados por furto de hardware. Consolidar isso numa solução é a forma mais barata e eficiente de garantir conformidade.

A Administração não está adstrita a uma definição acadêmica ou limitada do que compõe um EDR, mas sim ao que o mercado de alta performance oferece para suprir suas necessidades.

Reitera-se que o objeto da licitação não é definido unicamente pela nomenclatura "EDR", mas pela totalidade das exigências fixadas nos Anexos I e IV. O fato de o produto ser uma solução de segurança de *endpoint* avançada (EPP/XDR) que engloba criptografia apenas reforça a busca pela proposta mais vantajosa e eficiente, não havendo proibição legal para que o objeto contenha funcionalidades que extrapolem o conceito básico de detecção e resposta.

6. Da Console On-Premise (Item 3.1.1)

A alegação de que a exigência de console exclusivamente *on-premise* restringe a competitividade não deve prosperar, baseando-se nos seguintes preceitos:

- Soberania e Governança de Dados: A opção pela arquitetura *on-premise* constitui um padrão de segurança e governança estabelecido por esta Administração para garantir que o controle total sobre logs, telemetria e a infraestrutura de gestão permaneça sob domínio direto do órgão público. Tal escolha mitiga riscos de dependência exclusiva de nuvens de terceiros para operações críticas e assegura o cumprimento de políticas internas de segurança da informação.

- Continuidade Operacional e Proteção Offline: A especificação visa garantir a autonomia administrativa sob infraestrutura própria. O edital exige que a solução mantenha capacidade de proteção *offline* e que o gerenciamento fundamental (implantação de agentes, aplicação de políticas e coleta de logs) opere localmente, sem dependência de serviços externos para o funcionamento básico.

- Eficiência de Rede: O Termo de Referência exige que a solução possibilite a atualização das bases de dados (vacinas) e motores de segurança diretamente a partir da Console *On-Premise*. Isso permite que os milhares de *endpoints* da rede municipal se atualizem internamente, evitando o consumo excessivo e desnecessário da banda de internet do órgão, o que demonstra a observância ao Princípio da Eficiência e Economicidade.

- Modelo Híbrido Permitido: É importante ressaltar que o edital não veda o emprego de tecnologias em nuvem. A especificação admite a utilização de serviços *cloud* quando voltados à Inteligência de Ameaças Global (como reputação de arquivos, *cloud sandboxing* e telemetria avançada), desde que a gestão administrativa e o repositório principal de dados permaneçam locais.

- Garantia contra Obsolescência: O argumento de que o modelo afastaria soluções modernas é combatido pela vedação expressa, no Termo de Referência, ao fornecimento de soluções em regime de descontinuação (*End-of-Sale*, *End-of-Support* ou *End-of-Life*). A contratada é obrigada a manter o produto atualizado com as versões mais recentes durante toda a execução contratual.

7. Da Criação de Assinaturas HIPS (Item 1.5.2)

Diferente do que sustenta o impugnante, a capacidade de criação manual de regras de HIPS (Host Intrusion Prevention System) não representa obsolescência, mas sim uma funcionalidade crítica de Resposta a Incidentes (IR) e Threat Hunting.

- Complementaridade Tecnológica: Enquanto o *Machine Learning* e a Inteligência Artificial atuam na detecção de padrões e ameaças globais conhecidas, o HIPS provê ao analista de segurança a autonomia necessária para implementar Regras de Contenção Imediata.

- Ataques de Dia Zero (Zero-Day) e APTs: Em cenários de ameaças persistentes avançadas (APTs) direcionadas especificamente à

infraestrutura do órgão, a inteligência global dos fabricantes pode levar horas ou dias para processar e distribuir uma vacina automática. O HIPS permite a criação de uma 'assinatura de curtíssimo prazo' (vacina personalizada), bloqueando comportamentos específicos do ataque em andamento.

- Micro-segmentação e Defesa Adaptativa: Esta funcionalidade permite que o administrador neutralize vetores de ataque específicos (como o uso indevido de um processo legítimo do sistema) antes mesmo que o fabricante publique uma atualização oficial, garantindo a resiliência operacional e reduzindo drasticamente o *Mean Time to Remediate* (MTTR — Tempo Médio de Remediação).

8. Da Inexistência de Restrição à Competitividade (Art. 5º e 11, Lei 14.133/21)

O edital não restringe a competitividade, mas busca a proposta mais vantajosa e a eficiência administrativa.

O agrupamento das funcionalidades de segurança em um único item encontra respaldo no Princípio da Economicidade (Art. 5º da Lei nº 14.133/2021). A contratação fragmentada de soluções distintas (Antivírus, MDM, Firewall e Criptografia) imporia à Administração custos elevados e ineficientes de integração, múltiplos treinamentos especializados e manutenção complexa de diversos contratos. Além disso, a gestão pulverizada eleva o risco operacional em caso de descontinuidade de um dos fabricantes, enquanto a solução integrada garante a interoperabilidade nativa, essencial para a agilidade exigida pela tecnologia EDR na contenção de ameaças cibernéticas.

É imperativo destacar que diversos fabricantes líderes de mercado oferecem as funcionalidades exigidas de forma nativa e integrada em suas suítes de EPP/EDR. Portanto, a eventual ausência de determinadas camadas de proteção no portfólio específico de um licitante não pode compelir a Administração a reduzir o nível de segurança pretendido, sob pena de comprometer a eficiência da proteção dos ativos públicos e desconsiderar a necessidade devidamente motivada no Anexo Técnico.

Assim, considerando que as exigências são pertinentes, proporcionais e fundamentadas na convergência tecnológica atual, e que a fragmentação do objeto comprometeria a interoperabilidade e a segurança cibernética do Município

O edital não restringe a competitividade, mas busca a proposta mais vantajosa. O agrupamento de funções visa a interoperabilidade nativa e a economia de escala. A Administração não pode ser prejudicada pela limitação tecnológica de determinados portfólios, devendo prevalecer o interesse público na proteção rigorosa dos ativos e dados da Prefeitura de Joinville.

As soluções modernas de proteção de endpoint não se limitam a analisar arquivos, os argumentos apresentados pelo IMPUGNANTE remetem a soluções tecnicamente defasadas em relação às ameaças modernas e ao conceito de Defesa em profundidade.

A separação dessas funcionalidades em lotes distintos afrontaria o Princípio da Eficiência e o Princípio da Padronização, uma vez que a interoperabilidade e a gestão centralizada são requisitos críticos para a segurança cibernética do Município de Joinville.

As exigências contidas no edital e em seus anexos são pertinentes, proporcionais e fundamentadas na convergência tecnológica atual, visando o interesse público e a proteção integral dos dados da Prefeitura de Joinville.

Ante o exposto, decide-se pela IMPROCEDÊNCIA da impugnação, mantendo-se o certame em seus termos originais.

Sem mais, a Unidade de Governança e Contratações de TIC permanece à disposição para eventuais esclarecimentos necessários.

Assim, considerando a manifestação da secretaria requisitante do processo licitatório, a qual definiu as regras impugnadas, não assiste razão às alegações da Impugnante.

Diante do exposto, a impugnação apresentada não evidenciou nenhum fato que culminasse na reforma do Edital ora combatido, razão pela qual não merece provimento, mantendo-se inalteradas as disposições contidas no Edital.

V – DA CONCLUSÃO

Nesse contexto, verifica-se serem infundadas as razões ora apresentadas pela Impugnante, visto que não foram demonstradas irregularidades capazes de macular o procedimento licitatório, não insurgindo razões que impeçam a continuidade do edital de Pregão Eletrônico nº 092/2026.

VI – DA DECISÃO

Por todo o exposto, considerando as fundamentações aqui demonstradas e, principalmente, em homenagem aos princípios da legalidade, da razoabilidade e da eficiência, decide-se por conhecer da Impugnação e, no mérito, **INDEFERIR** as razões contidas na peça interposta pela empresa **NP SOLUÇÕES EM TI LTDA.**

Documento assinado eletronicamente por **Daniela Mezalira**, **Servidor(a) Público(a)**, em 03/03/2026, às 11:57, 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 **Silvia Cristina Bello**, **Diretor (a) Executivo (a)**, em 03/03/2026, às 16:45, 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 **Ricardo Mafra**, **Secretário (a)**, em 03/03/2026, às 16:50, 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 **28625994** e o código CRC **65C49F9A**.