

ESTUDO TÉCNICO PRELIMINAR

1. INFORMAÇÕES BÁSICAS:

1.1. O presente Estudo Técnico Preliminar tem por objeto a análise da necessidade, viabilidade e condições para a contratação de empresa especializada para disponibilização de licenças de uso de solução corporativa de proteção de endpoints, do tipo antivírus corporativo com recursos de EPP/EDR, destinadas ao atendimento da Prefeitura Municipal de Capão da Canoa/RS, abrangendo os órgãos, secretarias, setores administrativos, estações de trabalho, notebooks, servidores e demais equipamentos compatíveis que integrem o ambiente tecnológico do Poder Executivo Municipal.

1.2. A contratação deverá compreender o fornecimento de subscrição/licenciamento de software de segurança, incluindo direito de uso pelo período contratado, console centralizado de gerenciamento, implantação, configuração inicial, suporte técnico especializado, atualizações contínuas, upgrades, manutenção da solução e demais serviços necessários à plena operação da ferramenta no ambiente de Tecnologia da Informação da Prefeitura Municipal de Capão da Canoa/RS.

1.3. A solução pretendida deverá permitir a proteção integrada dos ativos tecnológicos municipais, com capacidade de prevenção, detecção, bloqueio, contenção e resposta a ameaças cibernéticas, tais como vírus, malwares, ransomwares, spywares, exploits, tentativas de invasão, arquivos maliciosos, comportamentos suspeitos e demais riscos relacionados à segurança da informação.

1.4. A contratação deverá contemplar, no mínimo, o fornecimento das licenças de uso da solução pelo prazo estimado de 36 (trinta e seis) meses, com gerenciamento centralizado por meio de console administrativa, preferencialmente em nuvem ou em modelo híbrido, permitindo à equipe de Tecnologia da Informação da Prefeitura realizar a aplicação de políticas de segurança, monitoramento do parque computacional, instalação e remoção de agentes, acompanhamento do status dos equipamentos protegidos, geração de alertas, emissão de relatórios técnicos e gerenciais, controle de atualizações e rastreabilidade das ações executadas.

1.5. A solução deverá contemplar suporte técnico durante toda a vigência contratual, atualizações automáticas das bases de detecção e dos componentes do produto, correções de segurança, disponibilização de novas versões, orientações técnicas para implantação e operação, bem como mecanismos de auditoria e comprovação da efetiva proteção dos equipamentos licenciados.

1.6. A contratação visa assegurar a continuidade dos serviços públicos municipais, a proteção dos dados institucionais e pessoais tratados pela Administração, a redução dos riscos de incidentes cibernéticos e a conformidade com a legislação aplicável, especialmente a Lei Federal nº 14.133/2021 e o Decreto Municipal nº 793/2023, sem prejuízo da observância da Lei Geral de Proteção de Dados — Lei Federal nº 13.709/2018, quando aplicável ao tratamento de dados pessoais pela Administração Pública.

1.7. A contratação caracteriza-se como solução comum de tecnologia da informação, de natureza contínua, necessária à manutenção da segurança, disponibilidade, integridade e confidencialidade dos ativos digitais da Prefeitura Municipal de Capão da Canoa/RS, devendo ser estruturada de forma a possibilitar ampla competitividade, admitindo-se solução de referência ou equivalente que atenda integralmente aos requisitos técnicos mínimos definidos nos instrumentos da contratação.

2. DESIGNAÇÃO DA EQUIPE DE PLANEJAMENTO:

2.1. Secretaria de Gestão, Inovação e Tecnologia.

2.2. Secretário Elisaldo Vieira Brehm

2.3. Servidores: Luis Otavio Alves de Carvalho.

3. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO:

3.1. A presente contratação decorre da necessidade de disponibilização de licenças de uso de solução corporativa de proteção de endpoints, do tipo antivírus corporativo com recursos de EPP/EDR, destinadas à Prefeitura Municipal de Capão da Canoa/RS, abrangendo os órgãos, secretarias, setores administrativos, estações de trabalho, notebooks, servidores e demais equipamentos compatíveis que integrem o ambiente tecnológico do Poder Executivo Municipal.

3.2. A infraestrutura de tecnologia da informação da Administração Municipal é essencial para a execução de serviços públicos, rotinas administrativas, tramitação de processos, atendimento ao cidadão, gestão de dados, comunicação institucional, arrecadação, emissão de documentos, acesso a sistemas internos e externos, execução de políticas públicas e suporte às atividades finalísticas das diversas secretarias municipais. Dessa forma, a indisponibilidade, perda, vazamento, sequestro ou comprometimento desses ativos digitais pode ocasionar prejuízos relevantes à continuidade dos serviços públicos e à eficiência da Administração.

3.3. A necessidade da contratação está diretamente relacionada à proteção do ambiente computacional da Prefeitura contra ameaças cibernéticas, tais como vírus, malwares, ransomwares, spywares, trojans, exploits, ataques de força bruta, arquivos maliciosos, acessos não autorizados, comportamentos suspeitos, movimentações laterais em rede e demais riscos que possam comprometer a confidencialidade, integridade, disponibilidade e autenticidade das informações públicas e dos dados pessoais tratados pelo Município.

3.4. A Administração Pública tem o dever de assegurar a continuidade, a eficiência e a segurança na prestação dos serviços públicos. A ausência de solução corporativa adequada de proteção de endpoints expõe o parque tecnológico municipal a incidentes de segurança capazes de paralisar sistemas, interromper atendimentos, comprometer bases de dados, afetar processos administrativos, gerar indisponibilidade de serviços essenciais e ocasionar custos extraordinários com recuperação de ambiente, contratação emergencial de suporte técnico, restauração de backups, horas extras de servidores e eventual responsabilização administrativa.

3.5. A contratação também se justifica pela necessidade de adoção de medidas preventivas e corretivas de segurança da informação, em conformidade com as boas práticas de governança de tecnologia da informação, bem como com os princípios da eficiência, planejamento, economicidade, segurança jurídica, interesse público, continuidade do serviço público e prevenção de riscos, observando-se a Lei Federal nº 14.133/2021 e o Decreto Municipal nº 793/2023, que orientam a adequada instrução da fase preparatória da contratação pública.

3.6. Além disso, a Prefeitura Municipal de Capão da Canoa/RS trata, armazena e processa dados institucionais e dados pessoais de cidadãos, servidores, fornecedores, contribuintes e usuários de serviços públicos. Assim, a contratação de solução de proteção endpoint contribui para o atendimento das obrigações previstas na Lei Geral de Proteção de Dados – LGPD, Lei Federal nº 13.709/2018, especialmente quanto à adoção de medidas técnicas e administrativas aptas a proteger dados pessoais contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

3.7. A solução atualmente pretendida deverá permitir a gestão centralizada da segurança dos equipamentos protegidos, possibilitando à equipe de Tecnologia da Informação do Município aplicar políticas de segurança, monitorar eventos, visualizar alertas, verificar o status de atualização dos agentes, identificar equipamentos desprotegidos, gerar relatórios, auditar ocorrências, executar ações de contenção e responder de forma mais rápida e estruturada a incidentes de segurança.

3.8. A utilização de soluções isoladas, desatualizadas ou sem gerenciamento centralizado não se mostra adequada ao contexto da Administração Municipal, pois dificulta a fiscalização, reduz a capacidade de resposta a incidentes, aumenta a exposição a vulnerabilidades, impede a padronização das políticas de segurança e compromete a rastreabilidade das ações executadas no ambiente tecnológico. Por essa razão, faz-se necessária a contratação de solução corporativa integrada, com licenciamento regular, suporte técnico, atualizações contínuas e console administrativa centralizada.

3.9. A necessidade também se fundamenta no caráter preventivo da contratação. A adoção de solução corporativa de antivírus/EDR representa medida de mitigação de riscos e de proteção do patrimônio público digital, tendo em vista que o custo de prevenção tende a ser significativamente inferior aos custos decorrentes de eventual incidente cibernético, como paralisação de sistemas, perda de produtividade, recuperação de dados, indisponibilidade de serviços, danos reputacionais, apuração de responsabilidades e adoção de medidas emergenciais.

3.10. Considerando o crescimento da complexidade das ameaças cibernéticas e a dependência cada vez maior dos serviços públicos em relação aos sistemas informatizados, a contratação revela-se necessária, adequada e proporcional ao atendimento do interesse público, pois visa elevar o nível de segurança da informação da Prefeitura Municipal de Capão da Canoa/RS, reduzir a superfície de ataque, proteger os ativos digitais municipais e garantir maior estabilidade, confiabilidade e continuidade às atividades administrativas e aos serviços prestados à população.

3.11. Dessa forma, a contratação de empresa especializada para disponibilização de licenças de solução corporativa de proteção de endpoints mostra-se indispensável para assegurar a proteção preventiva e corretiva do ambiente tecnológico municipal, com gerenciamento centralizado, suporte especializado, atualizações permanentes e recursos compatíveis com as necessidades da Administração, em observância à legislação aplicável e às diretrizes de planejamento, eficiência e segurança exigidas para as contratações públicas.

4. DESCRIÇÃO DOS REQUISITOS PARA A CONTRATAÇÃO:

4.1. A contratação deverá atender aos requisitos técnicos, operacionais, legais, administrativos e de segurança necessários à disponibilização de licenças de solução corporativa de proteção de endpoints, do tipo antivírus corporativo com recursos de EPP/EDR, destinadas à Prefeitura Municipal de Capão da Canoa/RS, observando-se a Lei Federal nº 14.133/2021, o Decreto Municipal nº 793/2023, a legislação municipal aplicável, as boas práticas de segurança da informação e, quando pertinente, a Lei Federal nº 13.709/2018 — Lei Geral de Proteção de Dados — LGPD.

4.2. A solução a ser contratada deverá ser compatível com o ambiente tecnológico da Prefeitura Municipal de Capão da Canoa/RS, abrangendo estações de trabalho, notebooks, servidores e demais equipamentos compatíveis utilizados pelos órgãos, secretarias e setores do Poder Executivo Municipal. Deverá permitir proteção contínua contra ameaças cibernéticas, gerenciamento centralizado, atualização permanente, suporte técnico especializado e comprovação da efetiva operação da ferramenta durante toda a vigência contratual.

4.3. A solução deverá consistir em plataforma corporativa de proteção de endpoints, compreendendo, no mínimo, funcionalidades de prevenção, detecção, bloqueio, contenção e resposta a ameaças, incluindo vírus, malwares, ransomwares, spywares, trojans, exploits, arquivos maliciosos, comportamentos suspeitos, acessos indevidos e demais riscos que possam comprometer a segurança, integridade, confidencialidade, disponibilidade e autenticidade das informações e dos ativos digitais municipais.

4.4. A contratação deverá contemplar o fornecimento de licenças/subscrições de uso da solução pelo prazo mínimo definido no instrumento convocatório, estimado em 36 (trinta e seis) meses, incluindo o direito de uso do software, console de gerenciamento, agentes de proteção, atualizações, upgrades, correções, suporte técnico, implantação, configuração inicial e demais recursos necessários ao pleno funcionamento da solução.

4.5. A solução deverá possuir console centralizada de gerenciamento, preferencialmente em nuvem ou em modelo híbrido, que permita à equipe de Tecnologia da Informação da Prefeitura, no mínimo:

- a) administrar todos os endpoints licenciados a partir de painel único de controle;
- b) aplicar políticas de segurança de forma individual, por grupo, setor ou unidade administrativa;
- c) realizar ou orientar a instalação, remoção e atualização dos agentes de proteção;
- d) visualizar o status dos equipamentos protegidos;
- e) identificar equipamentos sem proteção, desatualizados ou com falhas;
- f) monitorar eventos e alertas de segurança em tempo real ou em periodicidade adequada;
- g) gerar relatórios técnicos e gerenciais;
- h) controlar perfis e permissões de usuários administrativos;
- i) manter registros de auditoria e logs das ações executadas;
- j) acompanhar a conformidade das políticas aplicadas aos equipamentos.

4.6. A solução deverá possuir agente/cliente de proteção compatível com os sistemas operacionais utilizados pela Administração Municipal, especialmente Windows 11, sem prejuízo de compatibilidade com outras versões ou sistemas eventualmente existentes no parque tecnológico, desde que tecnicamente suportados pelo fabricante. O agente deverá operar de forma contínua, com atualização automática e com o menor impacto possível no desempenho dos equipamentos.

4.7. A solução deverá disponibilizar proteção em tempo real, atualização automática de bases de detecção, mecanismos de análise comportamental, bloqueio de ameaças conhecidas e desconhecidas, quarentena de arquivos suspeitos, varredura manual e programada, proteção contra ransomware e demais funcionalidades compatíveis com solução corporativa de segurança de endpoints.

4.8. Quando ofertada solução com recursos de EDR, esta deverá permitir, no mínimo, maior visibilidade sobre eventos de segurança, identificação de comportamentos anômalos, investigação de ocorrências, registro de evidências, análise de cadeia de ataque, contenção de ameaças e apoio à resposta a incidentes, de modo a reduzir o tempo de detecção, contenção e tratamento de possíveis ataques cibernéticos.

4.9. A contratada deverá realizar a implantação, instalação, ativação e configuração inicial da solução no ambiente da Prefeitura Municipal de Capão da Canoa/RS, abrangendo, no mínimo:

- a) disponibilização e ativação das licenças contratadas;
- b) criação ou configuração do console de gerenciamento;
- c) parametrização inicial das políticas de segurança;
- d) orientação ou execução da instalação dos agentes nos equipamentos definidos pela Administração;
- e) validação do funcionamento da solução;
- f) entrega de relatório técnico de implantação;
- g) comprovação da quantidade de endpoints protegidos;
- h) demonstração do status das licenças, atualizações e políticas aplicadas.

4.10. A contratada deverá prestar suporte técnico especializado durante toda a vigência contratual, por meio de canal formal de atendimento, com registro de chamados, acompanhamento das solicitações, prazos de resposta e escalonamento, conforme níveis de criticidade definidos no Termo de Referência ou no contrato. O suporte deverá abranger dúvidas operacionais, falhas de funcionamento, problemas de ativação, dificuldades de atualização, incidentes relacionados à solução e orientações técnicas para adequada utilização da ferramenta.

4.11. Todas as atualizações, upgrades, correções, novas versões, bases de assinaturas, motores de detecção, componentes de segurança e demais recursos necessários à manutenção da proteção deverão estar incluídos no valor contratado, sem cobrança adicional durante a vigência da licença.

4.12. A solução deverá permitir a geração e exportação de relatórios, em formato usualmente aceito, contendo, no mínimo, informações sobre:

- a) quantidade de endpoints licenciados;
- b) quantidade de endpoints protegidos e ativos;
- c) equipamentos desatualizados, inativos ou com falhas;
- d) status das atualizações;
- e) ameaças detectadas e medidas adotadas;
- f) políticas de segurança aplicadas;
- g) eventos relevantes de segurança;
- h) histórico de ocorrências;
- i) dados necessários à fiscalização contratual e auditoria interna.

4.13. A solução deverá atender a requisitos de segurança administrativa, incluindo autenticação para acesso ao console, segregação de perfis, controle de permissões, registro de ações administrativas, rastreabilidade, logs de auditoria e adoção de práticas que reduzam riscos de acesso indevido à ferramenta de gerenciamento.

4.14. A contratação deverá observar a proteção de dados e a segurança das informações tratadas no ambiente da Prefeitura. Quando houver tratamento de dados pessoais, a contratada deverá observar as disposições da Lei Federal nº 13.709/2018 — LGPD, adotando 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.

4.15. A contratada deverá garantir que a solução fornecida seja original, regular, licenciada, atualizada e apta ao uso institucional, vedado o fornecimento de licenças irregulares, expiradas, compartilhadas de forma indevida, incompatíveis com o uso governamental ou em desacordo com as condições estabelecidas pelo fabricante.

4.16. A solução ofertada deverá ser acompanhada de documentação técnica mínima, manuais ou orientações de uso, informações de acesso ao suporte, comprovação de licenciamento, comprovação da vigência das licenças, bem como demais documentos necessários à fiscalização, ao aceite e à gestão contratual.

4.17. O recebimento e o aceite da solução ficarão condicionados à comprovação da efetiva disponibilização das licenças, ativação do console, configuração inicial, instalação ou disponibilização dos agentes, funcionamento da solução e entrega dos relatórios de implantação, conforme critérios definidos no Termo de Referência.

4.18. O pagamento deverá ocorrer somente após a efetiva disponibilização, implantação e aceite da solução pelo fiscal do contrato, mediante comprovação de que o objeto foi entregue em conformidade com as especificações, quantidades, prazos e condições estabelecidas no instrumento contratual.

4.19. A solução deverá possibilitar a continuidade da proteção durante toda a vigência contratual, não sendo admitida interrupção indevida do direito de uso, suspensão de atualizações, indisponibilidade injustificada do console, ausência de suporte ou qualquer conduta que comprometa a fruição integral das licenças contratadas pela Administração.

4.20. A contratação deverá ser estruturada de modo a preservar a competitividade do certame, admitindo-se solução de referência ou equivalente, desde que a solução ofertada atenda integralmente aos requisitos técnicos mínimos, funcionalidades, níveis de segurança, prazos, suporte, compatibilidade e condições de execução estabelecidos no Estudo Técnico Preliminar, Termo de Referência, Edital e demais documentos do processo, em conformidade com a Lei Federal nº 14.133/2021.

4.21. Considerando a natureza do objeto, recomenda-se que a contratação seja realizada como solução única e integrada, compreendendo licenças, console de gerenciamento, implantação, configuração, suporte e atualizações, evitando-se o parcelamento indevido de componentes interdependentes que possam comprometer a compatibilidade técnica, a rastreabilidade, a responsabilização da contratada e a eficiência da gestão da segurança da informação.

4.22. Os requisitos aqui estabelecidos têm por finalidade assegurar que a Prefeitura Municipal de Capão da Canoa/RS disponha de solução corporativa adequada à proteção de seus ativos digitais, com gerenciamento centralizado, suporte contínuo, licenciamento regular, atualização permanente e capacidade de prevenção e resposta a incidentes cibernéticos, contribuindo para a continuidade dos serviços públicos, a economicidade, a eficiência administrativa e a segurança das informações institucionais.

5. LEVANTAMENTO DE MERCADO:

5.1. Em atendimento à fase preparatória da contratação, nos termos da Lei Federal nº 14.133/2021 e do Decreto Municipal nº 793/2023, foi realizado levantamento de mercado com o objetivo de identificar soluções disponíveis capazes de atender à necessidade da Prefeitura Municipal de Capão da Canoa/RS quanto à disponibilização de licenças de solução corporativa de proteção de endpoints, do tipo antivírus corporativo com recursos de EPP/EDR, incluindo gerenciamento centralizado, suporte técnico, atualizações contínuas e proteção contra ameaças cibernéticas.

5.2. O levantamento buscou avaliar alternativas tecnicamente aptas à proteção do ambiente tecnológico municipal, considerando a necessidade de prevenção, detecção, bloqueio, contenção e resposta a ameaças como vírus, malwares, ransomwares, spywares, exploits, arquivos maliciosos, comportamentos suspeitos e demais riscos que possam comprometer a confidencialidade, integridade, disponibilidade e autenticidade das informações públicas e dos dados pessoais tratados pela Administração.

5.3. Para fins de análise, foram considerados critérios técnicos, operacionais, econômicos e de aderência ao contexto da Administração Pública, especialmente:

- a) compatibilidade com o ambiente tecnológico da Prefeitura Municipal de Capão da Canoa/RS, em especial com estações de trabalho, notebooks e equipamentos com sistema operacional Windows 11;
- b) existência de console centralizado de gerenciamento, preferencialmente em nuvem ou em modelo híbrido;
- c) capacidade de aplicação de políticas de segurança em massa;
- d) proteção em tempo real contra malwares, ransomwares e demais ameaças cibernéticas;
- e) recursos de detecção e resposta a incidentes, preferencialmente com funcionalidades de EDR;
- f) geração de relatórios técnicos e gerenciais;
- g) controle de acesso, rastreabilidade e registros de auditoria;
- h) suporte técnico especializado durante toda a vigência contratual;
- i) atualizações e upgrades incluídos no licenciamento;
- j) compatibilidade com as obrigações de segurança da informação e proteção de dados pessoais;
- k) existência de precedentes de contratação no setor público;
- l) disponibilidade de parâmetros de preço em bases públicas;
- m) economicidade, vantajosidade e eficiência para a Administração.

5.4. No levantamento realizado, foram identificadas soluções corporativas de proteção de endpoints disponíveis no mercado, com diferentes níveis de complexidade, custo, recursos de segurança e maturidade de implantação em ambientes públicos. Entre as alternativas analisadas, destacam-se as seguintes:

5.5. Solução 1 — Kaspersky Next EDR Optimum Brazilian Edition

5.5.1. A solução Kaspersky Next EDR Optimum Brazilian Edition consiste em plataforma corporativa de proteção de endpoints, disponibilizada em modelo de subscrição/licenciamento, com recursos de proteção em tempo real, detecção de ameaças, resposta a incidentes, gerenciamento centralizado e atualizações contínuas. A solução permite a administração de múltiplos endpoints a partir de console centralizada, com aplicação de políticas de segurança, monitoramento de eventos, geração de relatórios e controle do estado de proteção dos equipamentos.

5.5.2. A solução apresenta aderência ao contexto da Prefeitura Municipal de Capão da Canoa/RS por contemplar funcionalidades compatíveis com as necessidades identificadas pela área de Tecnologia da Informação, especialmente quanto à proteção de estações de trabalho, notebooks, servidores e demais equipamentos compatíveis integrantes do parque tecnológico municipal.

5.5.3. A solução também se destaca por possuir histórico de adoção por órgãos e entidades públicas brasileiras, inclusive em contratações consultadas em bases públicas como o Portal Nacional de Contratações Públicas — PNCP e portais de controle externo, o que contribui para maior previsibilidade quanto à implantação, suporte e parametrização de preços de referência no âmbito da Administração Pública.

5.5.4. Além disso, a solução possui registros de bom desempenho em avaliações técnicas independentes de segurança corporativa, com análise de proteção, desempenho e usabilidade em cenários realistas de ameaças, o que fornece elemento técnico objetivo para subsidiar sua indicação como solução de referência.

5.6. Solução 2 — Microsoft Defender for Endpoint

5.6.1. O Microsoft Defender for Endpoint é solução de proteção de endpoints integrada ao ecossistema Microsoft, com recursos de detecção, resposta a incidentes e gerenciamento por meio de portais e ferramentas próprias da plataforma Microsoft.

5.6.2. A solução pode apresentar vantagens para organizações que já possuam ampla padronização no ecossistema Microsoft 365, especialmente em planos que contemplem recursos avançados de segurança. Contudo, sua utilização plena pode depender da contratação e manutenção de licenças específicas, como planos corporativos mais avançados, o que pode elevar o custo total de propriedade para a Administração quando não houver padronização integral nesse ambiente.

5.6.3. Também se observou que a adoção da solução pode demandar maior integração com ferramentas Microsoft complementares, como portal de segurança, gerenciamento de identidades e dispositivos, o que pode aumentar a complexidade operacional em ambientes heterogêneos ou com estrutura reduzida de equipe especializada.

5.7. Solução 3 — CrowdStrike Falcon

5.7.1. A plataforma CrowdStrike Falcon é solução de segurança de endpoints com recursos avançados de EDR/XDR, arquitetura em nuvem e forte capacidade de detecção e resposta a ameaças sofisticadas.

5.7.2. Trata-se de solução tecnicamente robusta, com presença significativa em ambientes corporativos de grande porte e organizações com estruturas especializadas de segurança da informação. Entretanto, no contexto municipal, pode apresentar custo de licenciamento superior ao de outras alternativas e maior exigência de maturidade operacional para plena utilização de seus recursos.

5.7.3. No levantamento realizado, verificou-se menor disponibilidade de precedentes de contratação por municípios de porte similar ao de Capão da Canoa/RS em bases públicas nacionais, o que reduz a previsibilidade quanto à implantação, ao suporte e à comparação de preços em ambiente público municipal.

5.8. Solução 4 — Sophos Intercept X

5.8.1. O Sophos Intercept X é solução corporativa de proteção de endpoints com recursos de prevenção contra ameaças, inteligência artificial, proteção contra ransomware, gerenciamento centralizado e funcionalidades de EDR em determinadas versões.

5.8.2. Embora possua boa reputação técnica no mercado de segurança da informação, verificou-se menor recorrência de contratações públicas municipais identificadas em bases abertas nacionais quando comparada à solução indicada como referência, o que pode dificultar a obtenção de parâmetros de preço e de experiências administrativas similares.

5.8.3. A solução pode atender tecnicamente a parte relevante das necessidades da Administração, desde que comprovada sua compatibilidade com o ambiente municipal, disponibilidade de suporte, atendimento aos requisitos mínimos e aderência integral às condições estabelecidas no Termo de Referência.

5.9. Solução 5 — Bitdefender GravityZone

5.9.1. O Bitdefender GravityZone é plataforma corporativa de proteção de endpoints com gerenciamento centralizado, proteção em tempo real, recursos de prevenção e resposta a ameaças, além de funcionalidades avançadas conforme a versão licenciada.

5.9.2. A solução apresenta avaliação positiva no mercado de segurança da informação e pode constituir alternativa tecnicamente viável, desde que observados os requisitos de compatibilidade, suporte, licenciamento, gerenciamento centralizado e proteção exigidos pela Administração.

5.9.3. Contudo, assim como outras soluções analisadas, foi identificada menor recorrência de contratações públicas municipais comparáveis em bases abertas nacionais, o que limita a formação de parâmetro público de preço e a previsibilidade de implantação no contexto específico da Prefeitura Municipal de Capão da Canoa/RS.

5.10. Após análise das alternativas disponíveis, verifica-se que a solução Kaspersky Next EDR Optimum Brazilian Edition apresenta melhor aderência às necessidades atualmente identificadas pela Prefeitura Municipal de Capão da Canoa/RS, especialmente por reunir proteção corporativa de endpoints, recursos de EPP/EDR, gerenciamento centralizado, atualizações contínuas, suporte técnico, precedentes de contratação pública e parâmetros de preço obtidos em contratações similares.

5.11. A indicação da solução Kaspersky como referência técnica não tem por objetivo restringir indevidamente a competitividade, mas sim conferir maior precisão à descrição do objeto, nos termos da Lei Federal nº 14.133/2021, especialmente quando necessária a padronização ou quando a indicação servir como referência para melhor compreensão do objeto. Assim, deverão ser admitidas soluções equivalentes ou superiores, desde que comprovem atendimento integral aos requisitos técnicos mínimos, funcionais, operacionais, de suporte, compatibilidade, segurança e desempenho definidos no Estudo Técnico Preliminar, Termo de Referência, Edital e demais documentos da contratação.

5.12. A escolha da solução de referência fundamenta-se nos seguintes elementos objetivos:

- a) compatibilidade com a necessidade de proteção do parque tecnológico da Prefeitura Municipal de Capão da Canoa/RS;
- b) disponibilidade de console centralizada de gerenciamento;
- c) capacidade de proteção contra malwares, ransomwares e ameaças avançadas;
- d) recursos de detecção, resposta, rastreabilidade e geração de relatórios;
- e) suporte técnico e atualizações incluídos durante a vigência do licenciamento;
- f) existência de precedentes de adoção por órgãos e entidades públicas;
- g) disponibilidade de amostras de preços em contratações públicas similares;
- h) aderência ao cenário de risco da Administração Municipal;
- i) melhor relação entre segurança, funcionalidade, previsibilidade de implantação e economicidade.

5.13. No aspecto econômico, a pesquisa preliminar de preços identificou contratações públicas similares, consultadas no LicitaCon e no Portal Nacional de Contratações Públicas — PNCP, resultando no valor unitário estimado de R\$ 219,76 (duzentos e dezenove reais e setenta e seis centavos) por licença individual para o período de 36 (trinta e seis) meses, valor utilizado como parâmetro estimativo para a presente contratação, sem prejuízo de eventual atualização, complementação ou saneamento da pesquisa de preços na fase própria do processo, conforme a legislação aplicável e as normas municipais de contratação pública.

5.14. Considerando o levantamento realizado, conclui-se que há pluralidade de soluções disponíveis no mercado aptas, em tese, a disputar o certame, desde que atendam aos requisitos mínimos estabelecidos pela Administração. Todavia, a solução Kaspersky Next EDR Optimum Brazilian Edition mostra-se, neste momento, a alternativa de referência mais aderente ao interesse público, por combinar desempenho técnico, viabilidade operacional, precedentes de contratação pública, gerenciamento centralizado, suporte, atualizações e compatibilidade com a necessidade de segurança da informação da Prefeitura Municipal de Capão da Canoa/RS.

5.15. Dessa forma, o levantamento de mercado demonstra a viabilidade da contratação e subsidia a definição da solução pretendida, observados os princípios do planejamento, eficiência, economicidade, seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração, competitividade, julgamento objetivo e interesse público, em conformidade com a Lei Federal nº 14.133/2021 e o Decreto Municipal nº 793/2023.

6. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO:

6.1. A solução pretendida consiste na contratação de empresa especializada para disponibilização de licenças de uso de solução corporativa de proteção de endpoints, do tipo antivírus corporativo com recursos de EPP/EDR, destinadas à Prefeitura Municipal de Capão da Canoa/RS, abrangendo os órgãos, secretarias, setores administrativos, estações de trabalho, notebooks, servidores e demais equipamentos compatíveis que integrem o ambiente tecnológico do Poder Executivo Municipal.

6.2. A contratação deverá compreender uma solução integrada de segurança da informação, contemplando, no mínimo, o fornecimento das licenças de uso, console centralizado de gerenciamento, agentes de proteção, implantação, ativação, configuração inicial, suporte técnico especializado, atualizações contínuas, upgrades, correções, manutenção da solução e demais recursos necessários à plena operação da ferramenta durante toda a vigência contratual.

6.3. A solução deverá ser disponibilizada em modelo de subscrição/licenciamento, pelo prazo estimado de 36 (trinta e seis) meses, assegurando à Administração o direito de uso regular da ferramenta durante todo o período contratado, incluindo as atualizações de bases de detecção, motores de análise, componentes de segurança, novas versões e correções disponibilizadas pelo fabricante, sem custos adicionais à Prefeitura Municipal de Capão da Canoa/RS.

6.4. A solução deverá atuar de forma preventiva, detectiva e corretiva, permitindo a proteção dos ativos digitais municipais contra ameaças cibernéticas conhecidas e desconhecidas, tais como vírus, malwares, ransomwares, spywares, trojans, exploits, arquivos maliciosos, comportamentos suspeitos, acessos indevidos, tentativas de invasão, movimentações laterais em rede e demais riscos que possam comprometer a confidencialidade, integridade, disponibilidade e autenticidade das informações tratadas pela Administração Pública Municipal.

6.5. A solução deverá possuir arquitetura corporativa de proteção de endpoints, com console centralizado de gerenciamento, preferencialmente em nuvem ou em modelo híbrido, permitindo à equipe de Tecnologia da Informação da Prefeitura administrar, monitorar e controlar os equipamentos protegidos por meio de painel único. A console deverá possibilitar a aplicação de políticas de segurança, visualização do status dos endpoints, monitoramento de alertas, geração de relatórios, identificação de equipamentos desprotegidos ou desatualizados, controle de perfis administrativos e rastreabilidade das ações executadas.

6.6. O gerenciamento centralizado é elemento essencial da solução, pois permitirá à Administração Municipal padronizar as políticas de segurança, reduzir a dependência de intervenções manuais em cada equipamento, melhorar a resposta a incidentes, ampliar a visibilidade sobre o parque computacional e facilitar a fiscalização contratual, mediante emissão de relatórios técnicos e gerenciais extraídos da própria ferramenta.

6.7. A solução deverá contemplar agentes de proteção compatíveis com o ambiente tecnológico da Prefeitura Municipal de Capão da Canoa/RS, especialmente com equipamentos que utilizem o sistema operacional Windows 11, sem prejuízo de compatibilidade com outras versões ou sistemas operacionais eventualmente existentes no parque municipal, desde que suportados tecnicamente pelo fabricante. Os agentes deverão operar de forma contínua, automática e transparente ao usuário final, com baixo impacto no desempenho dos equipamentos.

6.8. A solução deverá possibilitar a instalação, atualização e, quando tecnicamente viável, a remoção remota dos agentes de proteção, bem como a configuração de políticas de segurança em massa, por grupos, setores, unidades administrativas ou perfis de equipamentos, de modo a atender à organização interna da Prefeitura Municipal de Capão da Canoa/RS.

6.9. A solução deverá oferecer proteção em tempo real, varreduras programadas e sob demanda, quarentena de arquivos suspeitos, bloqueio de ameaças, análise comportamental, proteção contra ransomware, controle de eventos de segurança, registros de ocorrência e mecanismos de resposta, de forma a reduzir a superfície de ataque e mitigar riscos de interrupção dos serviços públicos municipais.

6.10. Os recursos de EDR, quando aplicáveis à versão contratada, deverão permitir maior capacidade de detecção e resposta a incidentes, possibilitando a identificação de comportamentos anômalos, investigação de eventos, visualização de evidências, análise da cadeia de ataque, contenção de ameaças e apoio à equipe de Tecnologia da Informação na adoção de medidas corretivas e preventivas.

6.11. A implantação da solução deverá ser realizada pela contratada, com acompanhamento da equipe técnica da Prefeitura, compreendendo, no mínimo:

- a) disponibilização e ativação das licenças contratadas;
- b) criação, liberação ou configuração da console de gerenciamento;
- c) parametrização inicial das políticas de segurança;
- d) orientação técnica ou execução da instalação dos agentes nos equipamentos definidos pela Administração;
- e) validação do funcionamento da solução;
- f) demonstração do painel de gerenciamento à equipe de TI;
- g) entrega de relatório técnico de implantação;
- h) comprovação do quantitativo de licenças disponibilizadas e endpoints protegidos;
- i) comprovação do status de atualização e das políticas aplicadas.

6.12. A contratada deverá prestar suporte técnico especializado durante toda a vigência contratual, por meio de canal formal de atendimento, com registro de chamados, prazos de resposta, acompanhamento das solicitações e escalonamento conforme a criticidade do problema. O suporte deverá abranger falhas de funcionamento, dificuldades de ativação, atualização, instalação, configuração, operação da console, dúvidas técnicas e incidentes relacionados à solução contratada.

6.13. A solução deverá permitir a emissão e exportação de relatórios técnicos e gerenciais que possibilitem à Administração acompanhar a execução contratual e a efetiva utilização das licenças, contendo, no mínimo, informações sobre endpoints licenciados, endpoints ativos, status de atualização, políticas aplicadas, ameaças detectadas, eventos relevantes, equipamentos com falha, equipamentos desprotegidos e demais dados necessários à fiscalização e auditoria.

6.14. A solução deverá observar requisitos de segurança administrativa, incluindo controle de acesso à console, autenticação de usuários autorizados, segregação de perfis, definição de permissões, registros de auditoria e logs de ações executadas, de forma a garantir rastreabilidade, transparência e controle sobre as operações realizadas no ambiente da Prefeitura.

6.15. A solução também deverá contribuir para o atendimento das obrigações legais relacionadas à segurança da informação e à proteção de dados pessoais, especialmente aquelas previstas na Lei Federal nº 13.709/2018 — Lei Geral de Proteção de Dados — LGPD, mediante adoção de medidas técnicas e administrativas aptas a proteger dados pessoais e informações institucionais contra acessos não autorizados, perda, destruição, alteração, comunicação indevida ou qualquer forma de tratamento inadequado.

6.16. A contratação deverá ser estruturada em conformidade com a Lei Federal nº 14.133/2021 e com o Decreto Municipal nº 793/2023, observando os princípios do planejamento, eficiência, economicidade, interesse público, segurança jurídica, julgamento objetivo, competitividade e seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração.

6.17. A solução deverá ser contratada de forma integrada, compreendendo licenças, console de gerenciamento, implantação, configuração, suporte técnico e atualizações, uma vez que tais componentes são tecnicamente interdependentes. O parcelamento desses elementos poderia gerar incompatibilidades, dificuldades de suporte, sobreposição de responsabilidades, fragilidade na fiscalização contratual e risco à continuidade da proteção do ambiente tecnológico municipal.

6.18. A indicação de solução de referência, quando utilizada nos documentos da contratação, terá por finalidade caracterizar o padrão técnico mínimo esperado e conferir maior precisão à descrição do objeto, sem prejuízo da possibilidade de aceitação de soluções equivalentes ou superiores, desde que comprovadamente atendam a todos os requisitos técnicos, funcionais, operacionais, de segurança, suporte, compatibilidade e desempenho definidos no Estudo Técnico Preliminar, Termo de Referência, Edital e demais anexos.

6.19. A solução, portanto, deverá assegurar à Prefeitura Municipal de Capão da Canoa/RS uma camada corporativa e centralizada de proteção cibernética, capaz de reduzir riscos de incidentes, ampliar a capacidade de resposta da equipe de TI, proteger dados e sistemas municipais, manter a continuidade dos serviços públicos e garantir maior confiabilidade ao ambiente digital utilizado pela Administração e pelos cidadãos.

6.20. Dessa forma, a solução como um todo compreende não apenas o fornecimento de licenças de antivírus corporativo, mas a disponibilização de um conjunto integrado de tecnologia, suporte, gerenciamento, atualização, implantação e monitoramento, indispensável à proteção preventiva e corretiva dos ativos digitais da Prefeitura Municipal de Capão da Canoa/RS durante toda a vigência contratual.

7. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS:

7.1. A estimativa das quantidades a serem contratadas foi definida com base na necessidade de proteção do parque tecnológico da Prefeitura Municipal de Capão da Canoa/RS, abrangendo os equipamentos utilizados pelos órgãos, secretarias, departamentos, unidades administrativas e demais setores vinculados ao Poder Executivo Municipal que demandem proteção por solução corporativa de antivírus/EDR.

7.2. A quantidade estimada corresponde a 2.000 (dois mil) licenças, destinadas à proteção de endpoints, compreendendo estações de trabalho, computadores, notebooks, servidores e demais equipamentos compatíveis que integrem o ambiente tecnológico municipal, estejam em uso ou venham a ser utilizados durante a vigência da contratação.

7.3. Para fins de dimensionamento, considera-se que cada licença corresponderá, em regra, à proteção de 1 (um) endpoint, entendido como equipamento físico ou virtual compatível com a solução, abrangendo os ativos computacionais da Administração Municipal que necessitem de proteção contra ameaças cibernéticas.

7.4. A quantidade de 2.000 (dois mil) licenças visa assegurar cobertura adequada ao ambiente tecnológico da Prefeitura Municipal de Capão da Canoa/RS, contemplando não apenas os equipamentos atualmente em operação, mas também eventual necessidade de reposição, substituição, redistribuição, ampliação do parque computacional, criação de novos postos de trabalho, reorganização administrativa, atendimento de unidades descentralizadas e demandas supervenientes durante a vigência contratual.

7.5. O quantitativo estimado busca evitar a existência de equipamentos sem proteção adequada, situação que poderia comprometer a segurança da informação, a integridade dos sistemas, a disponibilidade dos serviços digitais e a continuidade das atividades administrativas e finalísticas do Município.

7.6. A definição da quantidade observa os princípios do planejamento, eficiência, economicidade, razoabilidade e interesse público, em conformidade com a Lei Federal nº 14.133/2021 e com o Decreto Municipal nº 793/2023, buscando dimensionar a contratação de forma compatível com a real necessidade da Administração, sem subdimensionamento ou superdimensionamento injustificado.

7.7. A quantidade estimada deverá ser validada pela equipe técnica de Tecnologia da Informação da Prefeitura Municipal de Capão da Canoa/RS, mediante inventário, relatório técnico, memória de cálculo ou documento equivalente, a ser juntado aos autos do processo administrativo, demonstrando a correlação entre o número de licenças pretendidas e o número de equipamentos a serem protegidos.

7.8. A estimativa das quantidades fica assim estabelecida:

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANTIDADE	QTDE. MÍNIMA	VALOR UNITÁRIO	VALOR TOTAL
1	Solução corporativa de proteção de endpoints, do tipo antivírus corporativo com recursos de EPP/EDR, tendo como referência técnica a solução Kaspersky Next EDR Optimum Brazilian Edition Licença de 36 meses.	UNIDADE	2.000	120	R\$ 219,76	R\$ 439.520,00

7.9. Assim, a quantidade de 2.000 (dois mil) licenças mostra-se adequada para atender à demanda estimada da Prefeitura Municipal de Capão da Canoa/RS, garantindo proteção centralizada e contínua aos endpoints municipais durante a vigência contratual, sem prejuízo de eventuais ajustes devidamente justificados pela área técnica, caso identificada necessidade superveniente no curso da fase preparatória ou da execução contratual.

8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO:

8.1. A estimativa do valor da contratação foi elaborada com base em pesquisa de preços realizada em contratações públicas similares, utilizando-se como fontes de consulta o LicitaCon e o Portal Nacional de Contratações Públicas — PNCP, em conformidade com a Lei Federal nº 14.133/2021, com o Decreto Municipal nº 793/2023 e demais normas aplicáveis à fase preparatória das contratações públicas.

8.2. A pesquisa teve por finalidade identificar valores praticados pela Administração Pública em contratações de objeto semelhante, especialmente licenças de solução corporativa de proteção de endpoints, do tipo antivírus corporativo com recursos de EPP/EDR, contemplando direito de uso, suporte técnico, atualizações, gerenciamento centralizado e vigência compatível com a necessidade da Prefeitura Municipal de Capão da Canoa/RS.

8.3. Para a formação do preço estimado, foram consideradas contratações públicas compatíveis quanto à natureza do objeto, características técnicas da solução, unidade de fornecimento, prazo de vigência das licenças, condições de execução e similaridade com a demanda municipal. As fontes consultadas demonstram a existência de contratações públicas envolvendo soluções equivalentes ou similares de proteção corporativa de endpoints, permitindo a definição de parâmetro objetivo, rastreável e aderente ao mercado público.

8.4. A estimativa foi calculada considerando a necessidade de contratação de 2.000 (dois mil) licenças, conforme quantitativo estimado para atendimento do parque tecnológico da Prefeitura Municipal de Capão da Canoa/RS, ao valor unitário estimado de R\$ 219,76 (duzentos e dezenove reais e setenta e seis centavos) por licença.

8.5. Com base no referido valor unitário e no quantitativo estimado, o valor total estimado da contratação corresponde a R\$ 263.712,00 (duzentos e sessenta e três mil, setecentos e doze reais).

8.6. O valor unitário estimado de R\$ 219,76 foi obtido a partir da análise das pesquisas realizadas no LicitaCon e no PNCP, considerando contratações públicas similares e compatíveis com o objeto pretendido, de modo a refletir parâmetro de mercado adequado para a Administração Pública.

8.7. A utilização de pesquisas realizadas em bases públicas oficiais confere maior segurança, transparência e rastreabilidade à estimativa de preços, permitindo verificar a compatibilidade do valor estimado com os preços praticados em contratações públicas de objeto semelhante.

8.8. A estimativa ora apresentada possui caráter referencial para fins de planejamento da contratação, instrução do processo administrativo, verificação de disponibilidade orçamentária e definição dos parâmetros de aceitabilidade de preços, sem prejuízo de eventual atualização, complementação ou saneamento da pesquisa de preços, caso necessário, no curso da fase preparatória.

8.9. Assim, considerando o quantitativo estimado de 2.000 (dois mil) licenças, o valor unitário de R\$ 219,76 e o valor total estimado de R\$ 439.520,00, entende-se que a estimativa da contratação encontra-se devidamente fundamentada em pesquisa realizada em bases públicas oficiais, observando os princípios do planejamento, economicidade, eficiência, transparência, razoabilidade e seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração, nos termos da Lei Federal nº 14.133/2021 e do Decreto Municipal nº 793/2023.

9. JUSTIFICATIVA PARA PARCELAMENTO:

9.1. Para a presente contratação, não se recomenda o parcelamento do objeto em itens ou lotes distintos, considerando que a solução pretendida possui natureza integrada e interdependente, abrangendo licenças de uso de solução corporativa de proteção de endpoints, console centralizado de gerenciamento, implantação, configuração inicial, suporte técnico especializado, atualizações contínuas, upgrades, correções e demais recursos necessários à plena operação da ferramenta no ambiente tecnológico da Prefeitura Municipal de Capão da Canoa/RS.

9.2. A solução de proteção de endpoints, do tipo antivírus corporativo com recursos de EPP/EDR, depende de funcionamento conjunto e coordenado entre seus componentes, especialmente agentes instalados nos equipamentos, console de gerenciamento, políticas de segurança, bases de atualização, módulos de detecção, mecanismos de resposta, registros de eventos, relatórios e suporte técnico. A separação desses componentes em contratações distintas poderia comprometer a compatibilidade técnica, a eficiência operacional e a responsabilização pela execução do objeto.

9.3. O parcelamento, nesse caso, poderia gerar riscos relevantes à Administração, tais como incompatibilidade entre ferramentas, sobreposição ou ausência de funcionalidades, dificuldades na implantação, falhas de comunicação entre agentes e console, atraso na resposta a incidentes, fragmentação de responsabilidades, maior complexidade de fiscalização e aumento do custo administrativo de gestão contratual.

9.4. A contratação em solução única e integrada permite à Administração Municipal obter maior padronização das políticas de segurança, uniformidade na proteção dos equipamentos, centralização da gestão, rastreabilidade das ações, simplificação do suporte técnico e maior celeridade na identificação, contenção e tratamento de ameaças cibernéticas.

9.5. A centralização da responsabilidade em uma única contratada também favorece a fiscalização contratual, pois permite verificar, de forma objetiva, a efetiva disponibilização das licenças, o funcionamento da console, a instalação ou ativação dos agentes, a aplicação das políticas de segurança, a atualização da solução, o atendimento de suporte e a geração de relatórios técnicos e gerenciais.

9.6. Considerando que a Prefeitura Municipal de Capão da Canoa/RS necessita proteger seu parque tecnológico de forma contínua, padronizada e centralizada, o fracionamento do objeto poderia reduzir a eficiência da contratação e aumentar os riscos de falhas de segurança, especialmente em razão da necessidade de resposta rápida a incidentes e da proteção uniforme dos endpoints municipais.

9.7. A contratação integrada também se justifica pela necessidade de preservar a continuidade dos serviços públicos municipais, a segurança das informações institucionais, a proteção de dados pessoais tratados pela Administração e a adequada governança do ambiente de tecnologia da informação.

9.8. Assim, a reunião dos componentes em um único objeto não configura restrição indevida à competitividade, mas medida técnica necessária à adequada execução da solução pretendida, desde que o edital e o Termo de Referência admitam a participação de licitantes que ofertem solução equivalente ou superior, capaz de atender integralmente aos requisitos mínimos estabelecidos pela Administração.

9.9. A opção pelo não parcelamento observa o disposto na Lei Federal nº 14.133/2021 e no Decreto Municipal nº 793/2023, especialmente quanto aos princípios do planejamento, eficiência, economicidade, interesse público, julgamento objetivo e seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração.

9.10. Dessa forma, conclui-se que o não parcelamento do objeto é a alternativa tecnicamente mais adequada para a presente contratação, pois assegura integração nativa entre os componentes da solução, uniformidade operacional, facilidade de gestão e fiscalização, suporte unificado, redução de riscos de incompatibilidade e maior efetividade na proteção dos ativos digitais da Prefeitura Municipal de Capão da Canoa/RS.

10. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES:

10.1. A presente contratação possui relação direta com as demais estruturas, serviços e contratações de Tecnologia da Informação que dão suporte ao funcionamento dos sistemas, equipamentos, redes e serviços digitais da Prefeitura Municipal de Capão da Canoa/RS, uma vez que a solução corporativa de proteção de endpoints atuará de forma integrada ao ambiente tecnológico municipal.

10.2. Consideram-se contratações correlatas aquelas que, embora não integrem diretamente o objeto desta contratação, possuem relação funcional ou operacional com a solução pretendida, podendo influenciar sua implantação, funcionamento, desempenho, segurança ou fiscalização. Nesse contexto, destacam-se, entre outras:

- a) serviços de infraestrutura de rede, conectividade e internet;
- b) soluções de firewall, segurança de perímetro e controle de tráfego;
- c) serviços de suporte técnico de informática, help desk e manutenção de equipamentos;
- d) servidores físicos ou virtuais utilizados pela Administração;
- e) serviços de diretório, autenticação e controle de usuários, como Active Directory ou solução equivalente;
- f) soluções de backup, armazenamento e recuperação de dados;
- g) ferramentas de monitoramento, registro de eventos, logs ou SIEM, quando existentes;
- h) serviços de hospedagem, nuvem, datacenter ou infraestrutura correlata;
- i) contratos de aquisição, locação ou manutenção de computadores, notebooks e demais ativos de TI;
- j) sistemas administrativos, tributários, contábeis, educacionais, de saúde, protocolo, gestão documental e demais sistemas utilizados pelo Município.

10.3. A efetividade da solução de antivírus corporativo com recursos de EPP/EDR depende de condições mínimas do ambiente tecnológico, tais como conectividade adequada, permissões administrativas, compatibilidade com os sistemas operacionais utilizados, atualização dos equipamentos, disponibilidade de credenciais, políticas de rede, inventário de ativos e rotinas internas de suporte e manutenção.

10.4. Há interdependência operacional especialmente com as rotinas de infraestrutura e suporte de TI, pois a instalação dos agentes de proteção, a aplicação de políticas de segurança, o monitoramento dos equipamentos, a correção de falhas, a análise de alertas e o tratamento de incidentes exigem atuação coordenada entre a contratada e a equipe técnica da Prefeitura Municipal de Capão da Canoa/RS.

10.5. A contratação também se relaciona com as soluções de backup e recuperação de dados, uma vez que a proteção de endpoints constitui uma das camadas da estratégia de segurança da informação, não substituindo a necessidade de cópias de segurança, políticas de recuperação, controle de acesso, atualização de sistemas e demais medidas preventivas e corretivas adotadas pela Administração.

10.6. Da mesma forma, a solução de antivírus/EDR não substitui ferramentas de firewall, controle de perímetro, gestão de identidade, políticas de senhas, conscientização de usuários ou monitoramento de eventos, mas atua de forma complementar a essas medidas, compondo o conjunto de controles necessários à redução dos riscos de incidentes cibernéticos no ambiente municipal.

10.7. Para adequada implantação e funcionamento da solução, a Administração deverá promover alinhamento entre a área de Tecnologia da Informação, os gestores dos contratos correlatos e a contratada, especialmente quanto ao cronograma de implantação, liberação de acessos, janelas de manutenção, compatibilidade dos equipamentos, comunicação aos usuários, tratamento de conflitos com softwares preexistentes e validação da cobertura dos endpoints.

10.8. Eventuais contratos vigentes de suporte, manutenção de equipamentos, infraestrutura de rede, segurança de perímetro, backup ou administração de sistemas deverão ser observados durante a execução, a fim de evitar conflitos técnicos, sobreposição de responsabilidades, lacunas operacionais ou interrupções indevidas nos serviços públicos.

10.9. A existência de contratações correlatas ou interdependentes não impede a presente contratação, mas reforça a necessidade de planejamento integrado e atuação coordenada, de modo que a solução de proteção de endpoints seja implantada de forma segura, compatível e eficiente no ambiente tecnológico da Prefeitura Municipal de Capão da Canoa/RS.

10.10. Assim, conclui-se que a contratação pretendida é operacionalmente interdependente das demais estruturas e serviços de TI do Município, especialmente infraestrutura de rede, suporte técnico, controle de usuários, backup, servidores e segurança de perímetro, devendo sua implantação e execução ser acompanhadas pela equipe técnica municipal para assegurar compatibilidade, continuidade dos serviços, segurança da informação e efetividade da proteção contratada.

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

11.1. Registra-se que o Município não possui Plano de Contratações Anual (PAC) elaborado no exercício corrente, razão pela qual o objeto desta contratação não consta de PAC. Nos termos do art. 12, inciso VII, da Lei Federal nº 14.133/2021, “a partir de documentos de formalização de demandas, os órgãos responsáveis pelo planejamento de cada ente federativo poderão, na forma de regulamento, elaborar plano de contratações anual (...)”.

11.2. Quanto ao alinhamento com o planejamento, consigna-se que: (i) a fase preparatória deve compatibilizar-se com o PAC “sempre que elaborado”, conforme art. 18, caput, da Lei Federal nº 14.133/2021; e (ii) o Estudo Técnico Preliminar contempla a “demonstração da previsão da contratação no plano de contratações anual, sempre que elaborado”, nos termos do art. 18, § 1º, inciso II, do mesmo diploma. Assim, na inexistência de PAC, atende-se ao comando legal mediante o presente registro e, quando o PAC vier a ser elaborado, a contratação deverá observar o plano, o qual “deverá ser divulgado (...) e será observado pelo ente federativo na realização de licitações e na execução dos contratos” (art. 12, § 1º).

11.3. Por fim, registra-se que o prosseguimento da presente contratação fica condicionado à autorização da autoridade competente, entendida como “agente público dotado de poder de decisão”, nos termos do art. 6º, inciso VI, da Lei Federal nº 14.133/2021, a ser formalizada nos autos.

12. DEMONSTRAÇÃO DOS RESULTADOS PRETENDIDOS:

12.1. Com a presente contratação, pretende-se disponibilizar à Prefeitura Municipal de Capão da Canoa/RS solução corporativa de proteção de endpoints, do tipo antivírus corporativo com recursos de EPP/EDR, capaz de elevar o nível de segurança do ambiente tecnológico municipal, reduzir riscos de incidentes cibernéticos e assegurar maior proteção aos sistemas, dados, equipamentos e serviços digitais utilizados pela Administração Pública.

12.2. O principal resultado esperado é a proteção centralizada e contínua dos endpoints municipais, abrangendo estações de trabalho, computadores, notebooks, servidores e demais equipamentos compatíveis utilizados pelos órgãos, secretarias, departamentos e unidades administrativas do Poder Executivo Municipal.

12.3. A contratação deverá proporcionar maior capacidade de prevenção, detecção, bloqueio, contenção e resposta a ameaças cibernéticas, tais como vírus, malwares, ransomwares, spywares, exploits, arquivos maliciosos, comportamentos suspeitos, tentativas de acesso indevido e demais riscos que possam comprometer a confidencialidade, integridade, disponibilidade e autenticidade das informações institucionais.

12.4. Espera-se, ainda, a padronização da política de segurança dos equipamentos da Prefeitura, mediante utilização de console centralizado de gerenciamento, permitindo à equipe de Tecnologia da Informação aplicar políticas de proteção, monitorar alertas, acompanhar o status dos equipamentos, verificar atualizações, identificar falhas e gerar relatórios técnicos e gerenciais.

12.5. A solução deverá contribuir para a redução da exposição do Município a ataques cibernéticos, especialmente aqueles capazes de causar indisponibilidade de sistemas, interrupção do atendimento ao cidadão, sequestro de dados, perda de informações, paralisação de rotinas administrativas ou prejuízos à continuidade dos serviços públicos.

12.6. Entre os resultados pretendidos, destacam-se:

- a) proteção de 2.000 (dois mil) endpoints da Prefeitura Municipal de Capão da Canoa/RS, conforme quantitativo estimado;
- b) disponibilização de licenças regulares e válidas durante todo o período contratado;
- c) implantação e configuração inicial da solução no ambiente municipal;
- d) utilização de console centralizado para gerenciamento dos equipamentos protegidos;
- e) aplicação padronizada de políticas de segurança;
- f) atualização contínua das bases de detecção, componentes e versões da solução;
- g) redução de equipamentos desprotegidos, desatualizados ou sem monitoramento;
- h) melhoria da capacidade de identificação e resposta a incidentes;
- i) geração de relatórios para fiscalização, auditoria e acompanhamento da execução contratual;
- j) suporte técnico especializado durante toda a vigência da contratação;
- k) maior rastreabilidade das ações administrativas e dos eventos de segurança;
- l) fortalecimento da segurança da informação no âmbito do Poder Executivo Municipal.

12.7. A contratação também deverá contribuir para a proteção dos dados pessoais tratados pela Prefeitura, em alinhamento com a Lei Federal nº 13.709/2018 — Lei Geral de Proteção de Dados — LGPD, uma vez que a adoção de medidas técnicas de segurança auxilia na prevenção de acessos não autorizados, perda, alteração, destruição, comunicação ou difusão indevida de dados pessoais e informações institucionais.

12.8. Do ponto de vista operacional, espera-se maior eficiência na atuação da equipe de Tecnologia da Informação, uma vez que o gerenciamento centralizado da solução permitirá reduzir intervenções manuais, otimizar o tempo de resposta, facilitar o diagnóstico de falhas, acompanhar a situação do parque computacional e priorizar ações corretivas de forma mais organizada.

12.9. Do ponto de vista econômico, a contratação possui caráter preventivo, pois busca reduzir a probabilidade de custos extraordinários decorrentes de incidentes cibernéticos, tais como recuperação de sistemas, restauração de backups, contratação emergencial de serviços especializados, indisponibilidade de serviços, retrabalho administrativo e eventuais prejuízos decorrentes de perda ou comprometimento de dados.

12.10. Do ponto de vista institucional, a solução pretendida deverá fortalecer a governança de Tecnologia da Informação, proporcionando maior controle sobre os ativos digitais, melhor rastreabilidade dos eventos de segurança, maior previsibilidade na gestão de riscos cibernéticos e maior segurança na continuidade das atividades administrativas e finalísticas do Município.

12.11. A contratação deverá permitir que a Administração acompanhe objetivamente os resultados por meio de evidências extraídas da própria solução, tais como relatórios de endpoints protegidos, status de atualização, ameaças detectadas, políticas aplicadas, registros de eventos, chamados de suporte e demais informações necessárias à fiscalização contratual.

12.12. Assim, os resultados pretendidos com a contratação estão diretamente relacionados à continuidade dos serviços públicos, à proteção dos ativos digitais municipais, à segurança das informações, à redução dos riscos de incidentes, à conformidade com a legislação aplicável e ao atendimento do interesse público, em observância à Lei Federal nº 14.133/2021 e ao Decreto Municipal nº 793/2023.

13. PROVIDÊNCIAS PRÉVIAS AO CONTRATO:

13.1. Antes da formalização contratual e da efetiva implantação da solução, a Prefeitura Municipal de Capão da Canoa/RS deverá adotar providências administrativas, técnicas e operacionais necessárias para assegurar que a contratação ocorra de forma planejada, eficiente e compatível com o ambiente tecnológico municipal, em conformidade com a Lei Federal nº 14.133/2021, o Decreto Municipal nº 793/2023 e demais normas aplicáveis.

13.2. A Administração deverá consolidar o levantamento do parque tecnológico municipal, confirmando o quantitativo de 2.000 (dois mil) licenças estimadas para a contratação, mediante inventário, relatório técnico, planilha de controle, memória de cálculo ou documento equivalente elaborado pela área de Tecnologia da Informação.

13.3. O inventário deverá contemplar, sempre que possível, a identificação dos equipamentos a serem protegidos, incluindo estações de trabalho, computadores, notebooks, servidores e demais endpoints compatíveis utilizados pelos órgãos, secretarias, departamentos, unidades administrativas e setores vinculados ao Poder Executivo Municipal.

13.4. A área de Tecnologia da Informação deverá verificar previamente a compatibilidade dos equipamentos com a solução pretendida, especialmente quanto ao sistema operacional utilizado, requisitos mínimos de hardware, conectividade, permissões administrativas, políticas de rede, configurações de segurança e eventuais softwares que possam causar conflito com a solução de antivírus/EDR.

13.5. Deverá ser realizado saneamento prévio do ambiente tecnológico, quando necessário, abrangendo a remoção de antivírus conflitantes, regularização de equipamentos desatualizados, verificação de versões de sistema operacional, aplicação de atualizações críticas, revisão de permissões administrativas e identificação de equipamentos inativos, obsoletos ou sem necessidade de licenciamento.

13.6. A Administração deverá definir os responsáveis pelo acompanhamento da contratação, com a designação formal do gestor e do fiscal do contrato, bem como, quando necessário, dos respectivos substitutos, observando-se as atribuições de acompanhamento, fiscalização, comunicação com a contratada, registro de ocorrências, validação técnica e ateste da execução.

13.7. Também deverá ser indicado ponto focal técnico da área de Tecnologia da Informação, responsável por acompanhar a implantação da solução, apoiar a contratada na liberação de acessos necessários, validar a configuração inicial, conferir os relatórios de implantação e auxiliar na definição das políticas de segurança a serem aplicadas.

13.8. A Prefeitura deverá organizar previamente os acessos necessários à implantação e operação da solução, incluindo contas administrativas, perfis de usuários, permissões de acesso, regras de autenticação, segregação de funções e controles de segurança, de modo a preservar a rastreabilidade e evitar acessos indevidos ao console de gerenciamento.

13.9. Quando houver estrutura de diretório, domínio, Active Directory ou solução equivalente, a Administração deverá verificar a viabilidade de integração ou compatibilização com a solução contratada, especialmente para fins de implantação centralizada, organização dos equipamentos por grupos, aplicação de políticas e controle de usuários administrativos.

13.10. Deverá ser elaborado cronograma preliminar de implantação, preferencialmente por etapas, contemplando fase inicial de validação, instalação ou ativação progressiva dos agentes, expansão por secretarias ou unidades administrativas, verificação de funcionamento, correção de inconsistências e aceite final da implantação.

13.11. A Administração deverá avaliar a necessidade de realização de piloto técnico ou implantação inicial em grupo reduzido de equipamentos, com o objetivo de verificar compatibilidade, desempenho, comunicação com o console, aplicação de políticas, atualização dos agentes e eventual impacto operacional antes da expansão para todo o parque tecnológico.

13.12. Deverão ser definidas previamente as políticas iniciais de segurança a serem aplicadas aos endpoints municipais, incluindo regras de varredura, atualização, quarentena, notificações, tratamento de ameaças, geração de alertas, permissões administrativas, exceções justificadas e periodicidade de emissão de relatórios.

13.13. A Administração deverá preparar as unidades e usuários para a implantação, quando necessário, mediante comunicação interna sobre a instalação ou ativação da solução, eventuais janelas de manutenção, cuidados operacionais, possíveis impactos temporários e canais de contato para comunicação de falhas ou dúvidas.

13.14. Deverão ser estabelecidos os critérios objetivos de aceite da solução, incluindo, no mínimo, comprovação da disponibilização das licenças contratadas, ativação do console de gerenciamento, configuração inicial, instalação ou ativação dos agentes nos equipamentos definidos pela Administração, funcionamento da proteção, atualização da solução e entrega de relatório técnico de implantação.

13.15. A Administração deverá definir as evidências mínimas exigidas da contratada para fins de aceite, tais como relatório de licenças disponibilizadas, relação de endpoints protegidos, status de atualização, políticas aplicadas, telas ou relatórios extraídos do console, registro de eventuais falhas identificadas e comprovação do canal de suporte técnico.

13.16. Deverá ser previsto fluxo de comunicação entre a Administração e a contratada, com indicação de responsáveis, canais oficiais de atendimento, forma de abertura e acompanhamento de chamados, prazos de resposta, escalonamento de incidentes e registro das ocorrências durante a implantação e a vigência contratual.

13.17. A Prefeitura deverá verificar a existência de contratações correlatas ou interdependentes, tais como suporte técnico, infraestrutura de rede, firewall, backup, servidores, sistemas administrativos e serviços de conectividade, a fim de alinhar responsabilidades, evitar conflitos operacionais e assegurar a compatibilidade da solução com o ambiente existente.

13.18. Também deverá ser verificada a disponibilidade orçamentária e a adequada classificação da despesa, conforme a estrutura administrativa do Município, especialmente considerando que as licenças se destinam ao atendimento do parque tecnológico da Prefeitura Municipal de Capão da Canoa/RS.

13.19. Caso existam registros documentados de incidentes cibernéticos anteriores, recomenda-se sua juntada aos autos, com indicação, quando possível, das datas, impactos, providências adotadas e setores afetados, a fim de reforçar a motivação da contratação, a necessidade de proteção preventiva e a adequação da solução pretendida ao cenário de risco do Município.

13.20. Por fim, antes da formalização do contrato, deverão estar devidamente instruídos os documentos da fase preparatória, incluindo a justificativa da necessidade, estimativa de quantidades, estimativa de valor, requisitos técnicos, critérios de aceite, obrigações das partes, modelo de fiscalização e demais elementos necessários à adequada contratação, garantindo segurança jurídica, planejamento e transparência ao procedimento.

14. IMPACTOS AMBIENTAIS:

14.1. A presente contratação, por tratar da disponibilização de licenças de uso de solução corporativa de proteção de endpoints, do tipo antivírus corporativo com recursos de EPP/EDR, possui natureza predominantemente tecnológica e imaterial, não envolvendo obras, intervenções físicas, fabricação de equipamentos, aquisição direta de hardware ou geração significativa de resíduos pela própria execução do objeto.

14.2. Dessa forma, em regra, não se identificam impactos ambientais diretos relevantes decorrentes da contratação, uma vez que o objeto consiste no licenciamento, implantação, configuração, atualização e suporte de solução de software destinada à proteção dos ativos digitais da Prefeitura Municipal de Capão da Canoa/RS.

14.3. Ainda assim, podem existir impactos ambientais indiretos relacionados ao uso da infraestrutura de Tecnologia da Informação já existente, especialmente quanto ao consumo de energia elétrica por estações de trabalho, notebooks, servidores e demais equipamentos protegidos, bem como ao eventual aumento temporário de processamento durante rotinas de instalação, atualização, varredura, análise de arquivos e monitoramento de segurança.

14.4. Tais impactos indiretos são considerados baixos e compatíveis com a natureza do objeto, tendo em vista que a solução será implantada em equipamentos já pertencentes ou utilizados pela Administração Municipal, sem necessidade, em princípio, de aquisição de novos equipamentos exclusivamente para sua operação.

14.5. Como medida mitigadora, recomenda-se que a solução seja configurada de modo a otimizar o uso dos recursos computacionais, preferencialmente com agendamento de varreduras completas, atualizações e rotinas de maior consumo em horários de menor utilização dos equipamentos, reduzindo impacto operacional e consumo energético desnecessário.

14.6. Também deverá ser priorizada, sempre que possível, a implantação, configuração, monitoramento e suporte de forma remota, evitando deslocamentos desnecessários, impressões, consumo de materiais físicos e emissão de documentos em papel, em observância aos princípios da eficiência, economicidade e sustentabilidade administrativa.

14.7. A Administração deverá priorizar a tramitação digital dos documentos relacionados à contratação, à implantação, à fiscalização e ao acompanhamento da solução, mantendo relatórios, termos de aceite, registros de chamados, evidências de implantação e demais documentos preferencialmente em meio eletrônico.

14.8. A solução contratada deverá permitir a emissão de relatórios digitais e exportáveis, evitando a necessidade de impressão de documentos, salvo quando indispensável à instrução processual, fiscalização, auditoria ou exigência administrativa específica.

14.9. A contratação também poderá contribuir indiretamente para a sustentabilidade, na medida em que a proteção adequada dos endpoints auxilia na preservação da vida útil dos equipamentos, reduzindo riscos de comprometimento de sistemas, reinstalações recorrentes, perda de dados, paralisações, formatações desnecessárias e substituições prematuras de ativos tecnológicos.

14.10. Na hipótese de a implantação ou manutenção da solução evidenciar equipamentos obsoletos, incompatíveis ou sem condições de uso, eventual descarte de bens de informática deverá observar os fluxos administrativos próprios da Prefeitura Municipal de Capão da Canoa/RS e a legislação aplicável à destinação ambientalmente adequada de resíduos eletroeletrônicos.

14.11. Caso haja substituição futura de equipamentos de informática, caberá à Administração adotar providências para que o descarte ou desfazimento de bens ocorra de forma ambientalmente adequada, com observância das normas sobre resíduos sólidos, logística reversa, patrimônio público e demais regramentos aplicáveis, evitando descarte irregular de componentes eletrônicos.

14.12. A contratada, quando atuar diretamente na implantação, suporte ou manutenção da solução, deverá observar boas práticas ambientais, evitando impressões desnecessárias, deslocamentos sem necessidade, uso excessivo de materiais físicos e qualquer conduta que gere resíduos ou impactos ambientais incompatíveis com a natureza do objeto.

14.13. Considerando a natureza digital da contratação, não se vislumbra necessidade de estudo ambiental específico, licenciamento ambiental ou adoção de medidas mitigadoras complexas, sendo suficientes as providências de racionalização do uso de recursos, priorização de meios eletrônicos, configuração eficiente da solução e destinação adequada de eventual resíduo eletrônico decorrente de substituições de equipamentos.

14.14. Assim, conclui-se que os impactos ambientais da contratação são inexistentes ou de baixa relevância direta, limitando-se a efeitos indiretos associados ao uso regular da infraestrutura de TI já existente, os quais podem ser mitigados por meio de boas práticas de sustentabilidade, eficiência energética, gestão digital de documentos e destinação ambientalmente adequada de equipamentos eletroeletrônicos, em conformidade com a Lei Federal nº 14.133/2021, o Decreto Municipal nº 793/2023 e demais normas aplicáveis.

15. VIABILIDADE DA CONTRATAÇÃO:

15.1. Diante da análise realizada no presente Estudo Técnico Preliminar, conclui-se pela viabilidade técnica, operacional, econômica e jurídica da contratação de empresa especializada para disponibilização de 2.000 (dois mil) licenças de solução corporativa de proteção de endpoints, do tipo antivírus corporativo com recursos de EPP/EDR, destinadas à Prefeitura Municipal de Capão da Canoa/RS, abrangendo os órgãos, secretarias, departamentos, unidades administrativas, estações de trabalho, notebooks, servidores e demais equipamentos compatíveis integrantes do ambiente tecnológico municipal.

15.2. A contratação mostra-se tecnicamente viável, pois há soluções disponíveis no mercado capazes de atender às necessidades identificadas pela Administração Municipal, contemplando proteção em tempo real, prevenção e bloqueio de ameaças, recursos de detecção e resposta a incidentes, console centralizado de gerenciamento, aplicação de políticas de segurança, atualização contínua, geração de relatórios, suporte técnico especializado e rastreabilidade das ações executadas.

15.3. A solução pretendida é adequada ao cenário tecnológico da Prefeitura Municipal de Capão da Canoa/RS, especialmente diante da necessidade de proteção centralizada dos equipamentos utilizados na prestação de serviços públicos, na execução de rotinas administrativas, na guarda e tratamento de dados institucionais e pessoais, no acesso a sistemas internos e externos e na manutenção da continuidade das atividades municipais.

15.4. A viabilidade operacional também resta demonstrada, uma vez que a solução poderá ser implantada e gerenciada pela equipe de Tecnologia da Informação da Prefeitura, com apoio da contratada, mediante console centralizado, instalação ou ativação de agentes nos equipamentos, parametrização de políticas de segurança, acompanhamento de alertas, emissão de relatórios e acionamento de suporte técnico durante toda a vigência contratual.

15.5. A contratação contribui para reduzir riscos de incidentes cibernéticos, tais como infecção por malwares, ransomwares, spywares, exploits, arquivos maliciosos, acessos indevidos e demais ameaças capazes de comprometer a confidencialidade, integridade, disponibilidade e autenticidade das informações tratadas pela Administração. Dessa forma, a solução pretendida atua como medida preventiva e corretiva de segurança da informação, essencial à proteção dos ativos digitais municipais.

15.6. Do ponto de vista econômico, a contratação revela-se viável e compatível com os preços praticados no mercado público, considerando a pesquisa de preços realizada no LicitaCon e no Portal Nacional de Contratações Públicas — PNCP, que resultou no valor unitário estimado de R\$ 219,76 (duzentos e dezenove reais e setenta e seis centavos) por licença e no valor total estimado de R\$ 439.520 (quatrocentos e trinta e nove mil quinhentos e vinte reais) para o quantitativo de 2.000 (dois mil) licenças.

15.7. A contratação possui caráter preventivo e tende a gerar economicidade para a Administração, uma vez que o custo de disponibilização de solução corporativa de proteção de endpoints é significativamente inferior aos potenciais prejuízos decorrentes de incidentes cibernéticos, tais como paralisação de sistemas, perda ou sequestro de dados, indisponibilidade de serviços, contratação emergencial de suporte especializado, restauração de backups, horas extras

de equipe técnica, danos institucionais e eventual responsabilização administrativa.

15.8. A solução pretendida também se mostra juridicamente viável, desde que observados os requisitos da fase preparatória, a correta definição do objeto, a adequada estimativa de quantidades e valores, a justificativa técnica da necessidade, os critérios objetivos de aceitabilidade, as obrigações das partes, o modelo de fiscalização, as condições de recebimento e pagamento e os demais elementos exigidos pela Lei Federal nº 14.133/2021 e pelo Decreto Municipal nº 793/2023.

15.9. A contratação está alinhada aos princípios do planejamento, eficiência, economicidade, interesse público, segurança jurídica, transparência, julgamento objetivo e seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração, previstos na legislação aplicável às contratações públicas.

15.10. Também se verifica aderência da contratação às obrigações de segurança da informação e proteção de dados pessoais, especialmente diante da necessidade de adoção de medidas técnicas e administrativas aptas a proteger os dados tratados pela Prefeitura Municipal de Capão da Canoa/RS, em consonância com a Lei Federal nº 13.709/2018 — Lei Geral de Proteção de Dados — LGPD.

15.11. A contratação como solução integrada, contemplando licenças, console de gerenciamento, implantação, configuração inicial, atualizações, suporte técnico e manutenção da solução, mostra-se a alternativa mais adequada para assegurar compatibilidade técnica, padronização da proteção, centralização da gestão, facilidade de fiscalização, suporte unificado e maior efetividade na proteção dos endpoints municipais.

15.12. Não foram identificados óbices técnicos, operacionais, econômicos ou jurídicos que inviabilizem a contratação, desde que sejam observadas as providências prévias indicadas neste Estudo Técnico Preliminar, especialmente a confirmação do quantitativo de licenças, a adequada instrução da pesquisa de preços, a definição dos critérios de aceite, a designação de gestor e fiscal do contrato e a formalização das condições de execução no Termo de Referência.

15.13. Assim, considerando a necessidade pública demonstrada, a existência de soluções disponíveis no mercado, a compatibilidade técnica da solução pretendida, a estimativa de preço fundamentada em bases públicas oficiais, a relevância da proteção dos ativos digitais municipais e a observância da legislação aplicável, conclui-se pela viabilidade da contratação, recomendando-se o prosseguimento da fase preparatória e a elaboração dos demais instrumentos necessários à contratação.

Capão da Canoa/RS, 17 de agosto de 2026.

Elisaldo Vieira Brehm

Secretário de Gestão, Inovação e Tecnologia

Luiz Otavio Alves Carvalho

Servidor Público

Coleta de Preço

Orçamento 1:

Portal Nacional de Contratações Públicas Buscar no PNCP

Item nº 1

Descrição: CONFORME ITEM 3 DO EDITAL

Critério de julgamento: Menor preço Situação: Homologado Tipo: Serviço Categoria do item de leilão: Não se aplica

Incentivo produtivo básico: Não Benefício: Sem benefício Margem de preferência normal: Não Margem de preferência adicional: Não

Exigência de conteúdo nacional (CIIA-PAC): Não

Quantidade: 350 Unidade de medida: UN Valor unitário estimado: R\$ 285,00 Valor total estimado: R\$ 99.750,00

RESULTADO(S)

Ordem de classificação 1º Data do resultado da homologação: 02/12/2025 Situação: Informado

CNPJ/CPF ou Nº de identificação do fornecedor: 00.258.246/0001-68 [Consultar sanções e penalidades do fornecedor](#)

Nome ou razão social do fornecedor: SOLO NETWORK BRASIL S.A.

Indicador de subcontratação: Não Porte da empresa: Demais Código do país: BRA

Uso da margem de preferência: Não Uso do benefício ME/EPP: Não Uso do critério de desempate: Não

Quantidade homologada: 350 Valor unitário homologado: R\$ 214,16 Valor total homologado: R\$ 74.956,00

Percentual de desconto aplicado ao critério de julgamento: 0,0000%



3. ESPECIFICAÇÕES, QUANTITATIVOS E VALOR MÁXIMO PARA A CONTRATAÇÃO

LOTE	ITEM	DESCRIÇÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
01	01	Solução corporativa Kaspersky Next EDR Optimum Brazilian Edition. 250-499 User 3 year Código do Produto: KL4066KATTS	350 Licenças	R\$ 285,00 Por licença	R\$ 99.750,00

<https://pnpc.gov.br/pnpc-api/v1/orgaos/01450804000155/compras/2025/25/arquivos/1>

Orçamento 2:

Portal Nacional de Contratações Públicas Buscar no PNCP Entrar

Contratação de empresa especializada em fornecimento de Licença - 1 - Kaspersky Next EDR Foundations Brazilian Edition. 150-249 User 3 year Renewal License - Compre 2 anos Leve 3.

Item nº 1

Descrição: "Software" aplicação: Informática, tipo: client server suite, características adicionais: antivírus corporativo, atualização contínua e su- DEVE SER CONSIDERADO TODOS OS ANEXOS, EM ESPECIAL O ESTUDO TÉCNICO PRELIMINAR, TERMO DE REFERÊNCIA E MINUTA DE CONTRATO.

Critério de julgamento: Menor preço Situação: Homologado Tipo: Material Categoria do item de leilão: Não se aplica

Incentivo produtivo básico: Não Benefício: Participação exclusiva para ME/EPP Código NCM: 84714900 Margem de preferência normal: Não

Margem de preferência adicional: Não Exigência de conteúdo nacional (CIIA-PAC): Não

Quantidade: 180 Unidade de medida: Unidade Valor unitário estimado: R\$ 217,50 Valor total estimado: R\$ 39.150,00

RESULTADO(S)

Data do resultado da homologação: 16/01/2026 Situação: Informado

CNPJ/CPF ou Nº de identificação do fornecedor: 12.641.727/0001-37 [Consultar sanções e penalidades do fornecedor](#)

Nome ou razão social do fornecedor: FORT SECURE TECNOLOGIA LTDA

Indicador de subcontratação: Não Porte da empresa: ME Código do país: BRA

Uso da margem de preferência: Não Uso do benefício ME/EPP: Não Uso do critério de desempate: Sim

Fundamentação da aplicação de critério de desempate: Instrução normativa de critério de julgamento e/ou edital (Sorteio)

Quantidade homologada: 180 Valor unitário homologado: R\$ 217,50 Valor total homologado: R\$ 39.150,00

Percentual de desconto aplicado ao critério de julgamento: 0,0000%

Orçamento 3:


Portal Nacional de Contratações Públicas

Buscar no PNCP
Entrar

de Referência.

Item n° 1

Descrição: SOFTWARE ANTIVÍRUS COM SOLUÇÃO EDR, com licença de 36 (trinta e seis) meses, para a proteção cibernética dos sistemas da Prefeitura Municipal de Taquari/RS, conforme especificações técnicas e condições estabelecidas no Termo de Referência, Anexo I do edital.

Critério de julgamento: Menor preço **Situação:** Em andamento **Tipo:** Material **Categoria do item de leilão:** Não se aplica

Incentivo produtivo básico: Não **Benefício:** Participação exclusiva para ME/EPP **Margem de preferência normal:** Não **Margem de preferência adicional:** Não

Exigência de conteúdo nacional (CIIA-PAC): Não

Quantidade: 150 **Unidade de medida:** UN **Valor unitário estimado:** R\$ 241,27 **Valor total estimado:** R\$ 36.190,50

RESULTADO(S)

Ordem de classificação 1º **Data do resultado da homologação:** 17/11/1858 **Situação:** Informado

CNPJ/CPF ou N° de identificação do fornecedor: 35.898.517/0001-24 [Consultar sanções e penalidades do fornecedor](#)

Nome ou razão social do fornecedor: CONTEGO CONSULTORIA LTDA

Indicador de subcontratação: Não **Porte da empresa:** EPP **Código do país:** BRA

Uso da margem de preferência: Não **Uso do benefício ME/EPP:** Não **Uso do critério de desempate:** Não

Quantidade homologada: 150 **Valor unitário homologado:** R\$ 167,37 **Valor total homologado:** R\$ 25.105,50

Percentual de desconto aplicado ao critério de julgamento: 0,0000%

Orçamento 4:


Portal Nacional de Contratações Públicas

Buscar no PNCP
Entrar

Registro de preço: Não

Item n° 1

Descrição: LICENÇA ANTI-VIRUS KASPERSKY INTERNET 1 DISPOSITIVO

Critério de julgamento: Menor preço **Situação:** Homologado **Tipo:** Material **Categoria do item de leilão:** Não se aplica

Incentivo produtivo básico: Não **Benefício:** Não se aplica **Margem de preferência normal:** Não **Margem de preferência adicional:** Não

Exigência de conteúdo nacional (CIIA-PAC): Não

Quantidade: 1 **Unidade de medida:** UN **Valor unitário estimado:** R\$ 280,00 **Valor total estimado:** R\$ 280,00

RESULTADO(S)

Ordem de classificação 1º **Data do resultado da homologação:** 14/04/2026 **Situação:** Informado

CNPJ/CPF ou N° de identificação do fornecedor: 17.029.964/0001-65 [Consultar sanções e penalidades do fornecedor](#)

Nome ou razão social do fornecedor: ADRIANO SILVA ALVES -ME

Indicador de subcontratação: Não **Porte da empresa:** Demais **Código do país:** BRA

Uso da margem de preferência: Não **Uso do benefício ME/EPP:** Não **Uso do critério de desempate:** Não

Quantidade homologada: 1 **Valor unitário homologado:** R\$ 280,00 **Valor total homologado:** R\$ 280,00

Percentual de desconto aplicado ao critério de julgamento: 0,0000%