



## **MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

### **ESTUDO TÉCNICO PRELIMINAR – ETP 034/2026**

#### **1. INFORMAÇÕES BÁSICAS:**

**1.1.** Processo Interno nº 1211/2026 ID 108143.

#### **2. DESIGNAÇÃO DA EQUIPE DE PLANEJAMENTO:**

O Estudo Técnico Preliminar – ETP será elaborado conjuntamente por servidores da área técnica e requisitante. A equipe será composta por:

Jayne Costa da Silva, matrícula 38318;

Rafaela Santos Cerezoli, matrícula 43116;

Nathielly Amaral Silva, Matrícula 42962;

#### **3. DIRETRIZES QUE NORTEARÃO ESTE ETP:**

Normativas que fundamentam este ETP: IN SEGES 58/2022, Lei Federal nº 14.133/2021, Lei Federal nº 12.527/2011.

#### **4. DESCRIÇÃO DA NECESSIDADE**

Considerando a infraestrutura tecnológica do município de Cerejeiras, identificamos a necessidade de garantir níveis adequados de segurança, desempenho e escalabilidade para o parque tecnológico municipal. A demanda surge da obrigatoriedade de proteger 600 endpoints (estações de trabalho e servidores) contra ameaças cibernéticas modernas, assegurando a continuidade das atividades administrativas e operacionais de todas as secretarias e unidades administrativas.

##### **4.1. JUSTIFICATIVA DA NECESSIDADE**

A presente contratação justifica-se pela necessidade de fortalecimento da segurança da informação no âmbito do Município de Cerejeiras, considerando o cenário atual de riscos cibernéticos e as ocorrências já registradas no ambiente tecnológico municipal em razão da ausência de solução corporativa adequada de proteção contra ameaças digitais.

O parque tecnológico municipal é composto por aproximadamente 600 (seiscentos) equipamentos de informática, entre computadores (estações de trabalho), notebooks e servidores, distribuídos nas diversas Secretarias e unidades administrativas. A inexistência de ferramenta corporativa com recursos avançados de proteção contribuiu para a exposição do





## **MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

ambiente a códigos maliciosos, ocasionando instabilidades operacionais, comprometimento de arquivos e indisponibilidade temporária de sistemas internos, com impacto direto na continuidade dos serviços públicos.

O cenário atual de segurança cibernética é marcado pelo aumento significativo de ataques sofisticados, como ransomware, ataques direcionados e ameaças persistentes avançadas (APTs), os quais não são adequadamente mitigados por soluções antivírus tradicionais baseadas exclusivamente em assinaturas. Nesse contexto, torna-se tecnicamente indispensável a adoção de solução que contemple recursos avançados de prevenção, detecção e resposta a incidentes (EDR – Endpoint Detection and Response), incluindo monitoramento centralizado, análise comportamental, resposta automatizada, isolamento remoto de equipamentos comprometidos e geração de relatórios para auditoria e rastreabilidade.

Sob o aspecto legal, a contratação encontra respaldo na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que impõe à Administração Pública o dever de adotar medidas técnicas e administrativas aptas a proteger dados pessoais e dados sensíveis sob sua responsabilidade, especialmente nas áreas de saúde, educação, assistência social e arrecadação tributária. A ausência de controles de segurança compatíveis com o grau de risco envolvido pode ensejar responsabilização administrativa, civil e judicial, além de danos reputacionais ao Município.

A medida também se fundamenta nos princípios da eficiência, planejamento e economicidade previstos na Lei nº 14.133/2021, considerando que a solução proposta representa alternativa tecnicamente adequada e proporcional aos riscos identificados, garantindo melhor relação custo-benefício à Administração Pública.

Diante do exposto, a contratação de solução corporativa de proteção de equipamentos de informática com recursos avançados de prevenção, detecção e resposta a incidentes revela-se medida técnica indispensável para assegurar a continuidade dos serviços públicos, preservar a integridade, confidencialidade e disponibilidade das informações institucionais, mitigar riscos operacionais e garantir conformidade legal.

### **4.2. INTERESSE PUBLICO**

A implementação de solução avançada de segurança cibernética no Município de Cerejeiras atende diretamente ao interesse público, na medida em que visa assegurar a continuidade e a regularidade dos serviços prestados à população. A paralisação de sistemas informatizados por ataques virtuais compromete atendimentos em áreas essenciais, como saúde, educação,





## **MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

assistência social e arrecadação, afetando direitos fundamentais do cidadão. Assim, a adoção de mecanismos eficazes de proteção tecnológica constitui medida preventiva indispensável para evitar prejuízos coletivos e garantir o funcionamento ininterrupto da Administração Pública.

Sob a perspectiva do interesse público primário, a proteção do patrimônio informacional municipal revela-se igualmente essencial. Os dados e sistemas utilizados pelo Município sustentam a formulação e a execução de políticas públicas, além de armazenarem informações pessoais e sensíveis da população. A adoção de medidas técnicas robustas reforça o dever institucional de guarda e proteção dessas informações, em conformidade com a Lei nº 13.709/2018, prevenindo danos à coletividade e resguardando a confiança da sociedade na gestão pública.

Ademais, a centralização do gerenciamento da segurança em plataforma unificada promove maior eficiência administrativa, racionalizando recursos humanos e tecnológicos. Tal medida contribui para a economicidade, a padronização de procedimentos e a melhoria da governança em tecnologia da informação, assegurando que os recursos públicos sejam aplicados de forma planejada e responsável.

Por fim, a atuação preventiva e proativa na mitigação de riscos cibernéticos reduz a probabilidade de gastos emergenciais elevados decorrentes de incidentes graves, preservando o equilíbrio financeiro do Município. Dessa forma, a contratação pretendida não se limita a uma solução técnica, mas configura instrumento de proteção do interesse coletivo, da continuidade das políticas públicas e da estabilidade institucional.

### **5. ÁREA REQUISITANTE**

Secretaria Municipal de Administração e Planejamento – SEMAP.

### **6. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO**

Requisitos mínimos a serem observados:

6.1. A contratação deverá atender à necessidade de proteção integral do ambiente tecnológico municipal, atualmente composto por aproximadamente 600 (seiscentos) endpoints, entre estações de trabalho e servidores, distribuídos nas diversas secretarias e unidades administrativas. Os requisitos mínimos devem assegurar níveis adequados de segurança, disponibilidade, desempenho e escalabilidade, compatíveis com a criticidade das atividades desempenhadas pela Administração Pública.



## **MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

6.2. Deverá ser garantida a proteção contínua contra ameaças cibernéticas modernas, incluindo códigos maliciosos, ataques de ransomware, tentativas de invasão, exploração de vulnerabilidades e demais riscos que possam comprometer a integridade, a confidencialidade e a disponibilidade das informações institucionais. Os requisitos devem contemplar mecanismos capazes de identificar comportamentos anômalos, registrar eventos de segurança, permitir rastreabilidade de incidentes e viabilizar resposta tempestiva a ocorrências que possam impactar os serviços públicos.

6.3. Sob o aspecto normativo, a contratação deverá atender às exigências legais relacionadas à proteção de dados pessoais e dados sensíveis tratados pelo Município, em especial aquelas previstas na Lei nº 13.709/2018, garantindo a adoção de medidas técnicas e administrativas aptas a prevenir acessos não autorizados, vazamentos, perda ou destruição indevida de informações.

6.4. A solução deverá possuir plataforma corporativa de proteção de endpoints com recursos de Endpoint Detection and Response (EDR).

6.5. Deverá permitir gerenciamento centralizado de todos os endpoints protegidos por meio de console de administração baseada em nuvem (cloud) ou arquitetura híbrida, acessível via interface web segura.

6.6. A solução deverá possuir capacidade de proteção contra: Malware, Ransomware, Spyware, Rootkits, Exploração de vulnerabilidades e Ataques baseados em comportamento.

6.7. Deverá possuir mecanismos de detecção comportamental, utilizando inteligência artificial, machine learning ou análise heurística avançada.

6.8. Deverá permitir isolamento remoto de endpoint comprometido, possibilitando a contenção imediata de incidentes de segurança.

6.9. Deverá registrar e armazenar eventos de segurança e telemetria, permitindo rastreabilidade e análise de incidentes.

6.10. A solução deverá permitir geração de relatórios técnicos e gerenciais, incluindo: eventos de segurança, ameaças detectadas, equipamentos protegidos e status de atualização.

6.11. Deverá possuir atualização automática da base de assinaturas e mecanismos de detecção, sem necessidade de intervenção manual.

6.12. A solução deverá permitir aplicação centralizada de políticas de segurança, incluindo configuração remota dos agentes instalados nos endpoints.



## **MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

- 6.13. Deverá possuir proteção contra ransomware, com capacidade de bloqueio automático de comportamentos suspeitos.
- 6.14. Deverá permitir varredura sob demanda e em tempo real.
- 6.15. Deverá possuir proteção web, com bloqueio de URLs maliciosas e phishing.
- 6.16. Deverá possuir controle de dispositivos externos, como bloqueio ou monitoramento de mídias removíveis (USB).
- 6.17. A solução deverá permitir integração com diretórios corporativos, como Microsoft Active Directory, quando existente.
- 6.18. Deverá possuir baixo impacto de desempenho nos endpoints, não comprometendo a produtividade dos usuários.
- 6.19. Deverá ser compatível com os seguintes sistemas operacionais:  
Microsoft Windows 10 ou superior  
Microsoft Windows 11  
Microsoft Windows Server 2016 ou superior.
- 6.20. A solução deverá suportar gerenciamento de no mínimo 600 endpoints, com possibilidade de expansão futura.
- 6.21. A solução deverá incluir: atualizações, suporte técnico e manutenção durante toda a vigência contratual.
- 6.22. A solução deverá permitir implantação remota do agente de proteção nos equipamentos da rede.
- 6.23. O fornecedor deverá disponibilizar suporte técnico especializado, durante a vigência contratual, para apoio à implantação e operação da solução.
- 6.24. A solução ofertada deverá ser reconhecida em relatórios de análise de mercado de segurança da informação elaborados por instituições independentes, tais como Gartner, IDC ou Forrester, ou equivalentes.

## **7. LEVANTAMENTO DE MERCADO**

**7.1.** As diferentes soluções de mercado encontradas para a demanda são através de:

### **01) Desenvolvimento de Software Próprio**

O desenvolvimento de software próprio consiste na criação de uma ferramenta personalizada,





## **MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

concebida especificamente para atender às demandas do ambiente tecnológico do Município, considerando suas particularidades operacionais, estrutura de rede, políticas internas e fluxos administrativos. Essa alternativa pressupõe a constituição ou contratação de equipe técnica especializada em desenvolvimento seguro, segurança da informação, testes de vulnerabilidade, atualização contínua e suporte permanente.

Como principal vantagem, destaca-se a possibilidade de total customização da solução, alinhando funcionalidades às necessidades específicas da Administração Municipal, além de maior controle sobre o código-fonte, regras de detecção e políticas de segurança. Em tese, também pode proporcionar independência tecnológica em relação a fornecedores externos.

Entretanto, as desvantagens são significativamente relevantes. O desenvolvimento de ferramenta com capacidade de enfrentar ameaças cibernéticas modernas — como ransomware, exploits de dia zero e ataques baseados em comportamento — exige elevado investimento financeiro, equipe altamente especializada e atualização constante frente a um cenário global de ameaças em permanente evolução. Além disso, o tempo necessário para pesquisa, desenvolvimento, testes, validação e manutenção contínua tende a ser prolongado, ampliando o risco de exposição do ambiente durante esse período. Para um município de porte médio, essa alternativa apresenta alto risco técnico e financeiro, além de possível insuficiência de capacidade operacional para manter o nível de segurança exigido.

### **02) Aquisição de Licenciamento de Prateleira**

A aquisição de licenciamento de prateleira baseado em assinaturas tradicionais refere-se à contratação de soluções convencionais de antivírus que operam predominantemente por meio de banco de assinaturas (vacinas), realizando a detecção de ameaças já catalogadas previamente pelos fabricantes.

Entre as vantagens dessa alternativa, destacam-se o custo geralmente inferior em comparação com soluções mais avançadas, a facilidade de implantação e a ampla disponibilidade no mercado. Trata-se de modelo amplamente difundido, com implementação relativamente simples e baixo grau de complexidade técnica inicial.

Todavia, suas limitações técnicas são expressivas. Soluções baseadas exclusivamente em assinaturas possuem baixa efetividade contra ameaças novas ou variantes ainda não identificadas, especialmente ataques de ransomware sofisticados e técnicas de evasão modernas. A detecção tende a ser reativa, dependendo da atualização constante das bases de



## MUNICÍPIO DE CEREJEIRAS

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

dados, o que pode gerar janela de vulnerabilidade. Além disso, normalmente não contemplam recursos avançados de resposta a incidentes, análise comportamental ou contenção automatizada, o que reduz significativamente a capacidade de mitigar danos em tempo real. Diante do cenário atual de ciberameaças, essa alternativa pode não oferecer nível de proteção compatível com a criticidade do ambiente público municipal.

### **03) Aquisição de Solução EDR “Next-Generation”**

A aquisição de solução EDR (Endpoint Detection and Response) de próxima geração consiste na contratação de licenças de mercado que utilizam tecnologias avançadas, como Inteligência Artificial, Machine Learning e análise comportamental, para identificar padrões suspeitos, prevenir ataques e responder automaticamente a incidentes. Exemplos de fornecedores amplamente reconhecidos incluem Trend Micro, Kaspersky e Bitdefender.

Entre as principais vantagens estão a detecção proativa de ameaças desconhecidas, a capacidade de identificar comportamentos anômalos mesmo sem assinatura prévia, o isolamento automático de dispositivos comprometidos, a geração de alertas inteligentes e a possibilidade de investigação detalhada de incidentes. Essas soluções oferecem monitoramento centralizado, maior visibilidade do ambiente e resposta rápida, reduzindo significativamente o impacto de eventuais ataques. Também favorecem a conformidade com normas de proteção de dados, como a Lei nº 13.709/2018, ao incorporarem controles robustos de segurança.

Como desvantagem, destaca-se o custo mais elevado em comparação com antivírus tradicionais, além da necessidade de adequada parametrização e eventual capacitação da equipe interna para correta utilização das funcionalidades avançadas. Ainda assim, considerando o cenário atual de ameaças cibernéticas e a criticidade dos dados tratados pela Administração Pública, essa alternativa apresenta maior aderência técnica às necessidades institucionais e melhor relação entre risco e efetividade.

**7.2.** A análise comparativa das alternativas evidencia diferenças substanciais quanto à viabilidade técnica, ao nível de proteção oferecido e à aderência às necessidades do Município. O desenvolvimento de software próprio, embora permita customização integral e maior controle sobre regras e políticas internas, demanda estrutura técnica altamente especializada, investimentos contínuos em pesquisa e atualização frente à rápida evolução das ameaças cibernéticas, além de tempo considerável para maturação da ferramenta. Considerando a





## **MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

complexidade dos ataques atuais — como ransomware sofisticado e exploração de vulnerabilidades desconhecidas — essa alternativa apresenta elevado risco operacional e financeiro, especialmente para um ente municipal que não dispõe de equipe dedicada exclusivamente à engenharia de segurança ofensiva e defensiva.

Por sua vez, a aquisição de licenciamento tradicional baseado apenas em assinaturas (modelo de “vacinas”) representa solução de menor custo inicial e implantação simplificada. Contudo, sua eficácia é predominantemente reativa, limitada à identificação de ameaças previamente catalogadas. Em um cenário de ataques cada vez mais dinâmicos, com uso de técnicas de ofuscação e variações constantes de malware, essa abordagem não oferece capacidade satisfatória de detecção comportamental nem mecanismos robustos de resposta automatizada. Assim, embora seja financeiramente mais acessível, não se mostra plenamente compatível com a criticidade do ambiente tecnológico municipal nem com o volume de endpoints a serem protegidos.

Em contraste, a Aquisição de Solução EDR “Next-Generation” demonstra maior alinhamento técnico e estratégico às necessidades identificadas. Plataformas dessa natureza, amplamente disponibilizadas por fornecedores consolidados no mercado como Trend Micro, Kaspersky e Bitdefender, utilizam Inteligência Artificial, Machine Learning e análise comportamental para identificar padrões suspeitos, inclusive ameaças desconhecidas ou de dia zero. Além da prevenção, incorporam recursos de detecção e resposta a incidentes (EDR), possibilitando isolamento automático de máquinas comprometidas, rastreabilidade de eventos e mitigação rápida de impactos.

Sob o ponto de vista da governança e do interesse público, essa alternativa oferece maior resiliência operacional, reduz o risco de paralisação de serviços essenciais e contribui para o cumprimento das obrigações legais relacionadas à proteção de dados pessoais, especialmente em consonância com a Lei nº 13.709/2018. Embora envolva investimento superior às soluções tradicionais, apresenta melhor relação entre custo e benefício quando analisado o potencial de prejuízos decorrentes de incidentes graves.

Diante da análise técnica, operacional e jurídica das alternativas, conclui-se que a Aquisição de Solução EDR “Next-Generation” constitui a opção mais adequada para atender às necessidades do Município, garantindo maior nível de proteção, resposta eficaz a incidentes, continuidade dos serviços públicos e preservação do patrimônio informacional.





## **MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

### **8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO**

A solução consiste na contratação de plataforma corporativa de proteção avançada para endpoints, abrangendo aproximadamente 600 (seiscentos) dispositivos, entre estações de trabalho e servidores do Município de Cerejeiras, com cobertura integral das secretarias e unidades administrativas. A ferramenta deverá operar de forma centralizada, permitindo gerenciamento unificado, aplicação padronizada de políticas de segurança, monitoramento contínuo e geração de relatórios técnicos e gerenciais para apoio à tomada de decisão.

A solução deverá contemplar mecanismos modernos de prevenção, detecção e resposta a incidentes (EDR), utilizando tecnologias como análise comportamental, inteligência artificial e aprendizado de máquina, capazes de identificar ameaças conhecidas e desconhecidas, inclusive ataques de ransomware e tentativas de exploração de vulnerabilidades. Deverá possibilitar resposta automatizada a incidentes, isolamento de dispositivos comprometidos, rastreabilidade de eventos e suporte à investigação técnica, garantindo maior resiliência ao ambiente tecnológico municipal.

O escopo da contratação deverá incluir a disponibilização das licenças necessárias, atualizações automáticas, suporte técnico especializado durante a vigência contratual e compatibilidade com a infraestrutura existente, assegurando desempenho adequado sem comprometer a produtividade dos usuários. A solução deverá permitir escalabilidade futura, caso haja ampliação do parque tecnológico municipal.

Sob o aspecto normativo, a implementação deverá contribuir para o fortalecimento da governança em segurança da informação e para o atendimento às exigências da Lei nº 13.709/2018, garantindo a adoção de medidas técnicas aptas a proteger dados pessoais e sensíveis tratados pela Administração Pública.

De forma integrada, a solução visa assegurar a continuidade dos serviços públicos, reduzir riscos operacionais, proteger o patrimônio informacional do Município e promover maior estabilidade, eficiência e segurança no ambiente tecnológico institucional.

### **9. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS**

A solução de segurança a ser contratada deverá contemplar a proteção dos equipamentos que compõem o ambiente tecnológico da Administração Municipal, incluindo estações de trabalho (desktops) e servidores que operam com sistema operacional Microsoft Windows Server.



## **MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

A ferramenta deverá oferecer proteção antivírus e recursos avançados de detecção e resposta a ameaças cibernéticas, abrangendo tanto os computadores utilizados pelos usuários quanto os servidores responsáveis pela execução de sistemas institucionais e armazenamento de informações.

A solução deverá ser compatível com os sistemas operacionais utilizados nas estações de trabalho e com o ambiente Microsoft Windows Server existente nos servidores, permitindo gerenciamento centralizado, atualização automática das bases de proteção e monitoramento contínuo do ambiente tecnológico.

Para fins de dimensionamento da contratação, estima-se a necessidade de licenciamento para os seguintes equipamentos do parque tecnológico municipal:

Estações de trabalho (desktops): 590 unidades

Servidores com sistema operacional Windows Server: 10 unidades

### **10. ESTIMATIVA DO VALOR DA CONTRATAÇÃO**

**10.1.** Os demonstrativos da estimativa do valor da contratação, acompanhados dos preços unitários (Pesquisa de Mercado), das memórias de cálculo constarão nos Autos do Processo Administrativo Digital Nº 1211/2026.

### **11. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO**

A solução não será parcelada em lotes, considerando a necessidade de integração, padronização e gerenciamento centralizado do ambiente de segurança da informação do Município. A contratação de plataforma única para proteção dos aproximadamente 600 endpoints garante uniformidade tecnológica, interoperabilidade entre os componentes e aplicação homogênea das políticas de segurança em todas as secretarias e unidades administrativas.

O parcelamento poderia resultar na adoção de soluções distintas, com consoles de gerenciamento independentes, políticas divergentes e possíveis incompatibilidades técnicas, comprometendo a eficiência operacional e ampliando a complexidade de administração. Tal fragmentação dificultaria o monitoramento centralizado, a correlação de eventos de segurança e a resposta coordenada a incidentes, reduzindo a efetividade da estratégia de proteção cibernética municipal.

Além disso, a contratação em lote único favorece a economicidade, ao possibilitar ganho de





## **MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

escala na aquisição das licenças e simplificação contratual, reduzindo custos administrativos e riscos de sobreposição de responsabilidades entre fornecedores distintos. Também contribui para maior clareza na definição de obrigações, níveis de serviço e suporte técnico, assegurando responsabilidade integral do contratado pelo funcionamento da solução.

## **12. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES**

Não há contratações correlatas e/ou interdependentes.

## **13. ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO**

**13.1.** A presente aquisição não tem previsão no Plano Anual de Contratação – PAC, entretanto tem no PPA, LOA e LDO.

A contratação não consta no Plano de Contratações Anual considerando o agravamento do cenário de crimes cibernéticos e à necessidade urgente de adequação à LGPD detectada após o planejamento inicial. Trata-se de uma medida corretiva e estratégica para evitar danos maiores e garantir a segurança do ambiente tecnológico da rede municipal.

## **14. RESULTADOS PRETENDIDOS**

A contratação visa fortalecer a segurança da informação no Município de Cerejeiras, garantindo maior proteção ao parque tecnológico e assegurando a continuidade dos serviços públicos. Os resultados pretendidos estão alinhados ao interesse público e ao cumprimento das exigências da Lei nº 13.709/2018, especialmente quanto à proteção de dados pessoais e sensíveis.

### **1. Continuidade dos Serviços Públicos**

- Redução do risco de paralisação de sistemas essenciais.
- Maior disponibilidade das plataformas utilizadas pelas secretarias.

### **2. Reforço da Segurança da Informação**

- Proteção mais eficaz contra ameaças cibernéticas modernas.
- Monitoramento contínuo e resposta mais rápida a incidentes.

### **3. Proteção de Dados e Governança**

- Preservação da integridade e confidencialidade das informações institucionais.
- Centralização do gerenciamento de segurança, com maior eficiência administrativa.

### **4. Racionalização de Custos**

- Redução da probabilidade de gastos emergenciais com incidentes.
- Melhor previsibilidade e aplicação dos recursos públicos.





## **MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

Com isso, busca-se consolidar um ambiente tecnológico mais seguro, estável e resiliente, assegurando suporte adequado às políticas públicas e ao atendimento à população.

### **15. PROVIDÊNCIAS A SEREM ADOTADAS**

Inicialmente, deverá ser realizado o levantamento atualizado dos equipamentos que serão contemplados, organizando a implantação de forma planejada para não prejudicar o funcionamento das secretarias e demais unidades administrativas. Também deverá ser designado servidor responsável pelo acompanhamento e fiscalização do contrato.

Durante a execução, será necessário estabelecer rotinas básicas de monitoramento, controle de acesso e acompanhamento dos relatórios de segurança, garantindo que o ambiente permaneça protegido e estável. A equipe de TI deverá receber as orientações necessárias para utilização adequada da ferramenta.

Por fim, deverão ser feitas avaliações periódicas para verificar o funcionamento da solução e a efetividade da proteção, assegurando a continuidade dos serviços públicos e o atendimento às exigências da Lei nº 13.709/2018.

### **16. POSSÍVEIS IMPACTOS AMBIENTAIS**

A contratação voltada à proteção do ambiente tecnológico municipal apresenta impactos ambientais indiretos, sobretudo relacionados ao consumo de energia elétrica pelos equipamentos de informática e à eventual substituição ou atualização de dispositivos ao longo do tempo. Embora se trate de solução predominantemente digital, a ampliação ou intensificação do uso de recursos tecnológicos pode contribuir para maior demanda energética e geração futura de resíduos eletroeletrônicos.

No entanto, tais impactos tendem a ser de baixa magnitude, considerando que a implementação ocorrerá sobre a infraestrutura já existente, sem necessidade de aquisição significativa de novos equipamentos. Ainda assim, é recomendável a adoção de boas práticas de gestão ambiental, como o uso racional de energia, a configuração adequada dos equipamentos para evitar consumo excessivo e o descarte ambientalmente adequado de componentes eletrônicos, em conformidade com a legislação pertinente.

Como medida mitigadora, o Município deverá priorizar políticas internas de sustentabilidade, promovendo a conscientização quanto ao uso eficiente dos recursos tecnológicos e garantindo que eventuais resíduos eletrônicos sejam destinados a empresas especializadas em reciclagem e logística reversa. Dessa forma, assegura-se que a contratação atenda ao interesse público não



**MUNICÍPIO DE CEREJEIRAS**

Prefeitura Municipal

Rua Florianópolis, nº 503 - Bairro Maranata, CEP 76.997-000

apenas sob o aspecto da segurança da informação, mas também sob a perspectiva da responsabilidade ambiental e da gestão sustentável.

**17. DECLARAÇÃO DE VIABILIDADE**

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

**Jayne Costa da Silva**

Decreto Nº 556/2025

Coordenadora do Setor de Contratações

**Rafaela Santos Cerezoli**

Decreto Nº 554/2025

Coordenadora de Processos Administrativos

**Nathielly Amaral Silva**

Decreto Nº 116/2025

Assessora de Departamento

**Dieferson Costa da Silva**

Decreto N.º 164/2023

Coordenador/Gestão de Tecnologia da Informática



# Município de Cerejeiras

04.914.925/0001-07  
Rua Florianópolis  
www.cerejeiras.ro.gov.br

## FICHA CADASTRAL DO DOCUMENTO ELETRÔNICO

Tipo do Documento	Identificação/Número	Data
<b>Estudo Técnico Preliminar- ETP</b>	<b>Nº 043/2026</b>	<b>06/03/2026</b>

ID: <b>830595</b>	Processo	Documento
CRC: <b>967697F7</b>		
Processo: <b>1-1211/2026</b>		
Usuário: <b>Rafaela Santos Cerezoli</b>		
Criação: <b>06/03/2026 07:49:18</b>	Finalização: <b>06/03/2026 07:49:18</b>	

MD5: <b>7113D8DBE953714F199AA18D6FF75CC9</b>
SHA256: <b>CA004EF40313A121382FA10E4E651E80BB8CCEE330E0DE3792A4DFD2721CB7FF</b>

Súmula/Objeto:

**Estudo Técnico Preliminar- ETP**

### INTERESSADOS

Secretaria Municipal de Administração e Planejamento	CEREJEIRAS	RO	06/03/2026 07:49:18
------------------------------------------------------	------------	----	---------------------

### ASSUNTOS

ANTIVIRUS	06/03/2026 07:49:18
-----------	---------------------

### ASSINATURAS ELETRÔNICAS

	Rafaela Santos Cerezoli	COORDENADOR DE PROCESSOS ADMINISTRATIVOS	06/03/2026 07:49:52
Assinado na forma do Decreto Municipal nº 284/2021.			
	NathIELly Amaral Silva	ASSESSOR DE DEPARTAMENTO	06/03/2026 07:51:48
Assinado na forma do Decreto Municipal nº 284/2021.			
	Jayne Costa da Silva	Coordenadora do Setor de Contratações	06/03/2026 07:52:24
Assinado na forma do Decreto Municipal nº 284/2021.			
	Dieferson Costa da Silva	Coordenador/Gestão de Tecnologia da Informática	06/03/2026 08:35:40
Assinado na forma do Decreto Municipal nº 284/2021.			

A autenticidade deste documento pode ser conferida através do QRCode acima ou ainda através do site [transparencia.cerejeiras.ro.gov.br](http://transparencia.cerejeiras.ro.gov.br) informando o ID 830595 e o CRC 967697F7.