Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

ESTUDO TÉCNICO PRELIMINAR

Orgão: Câmara Municipal de Cachoeiro de Itapemirim
Setor Requisitante: TI - Tecnologia da Informação
Processo Administrativo nº: 19.175 / 2026

O Estudo Técnico Preliminar – ETP constitui instrumento integrante da fase preparatória das contratações públicas, destinado a caracterizar a necessidade administrativa e subsidiar a definição da solução mais adequada ao atendimento do interesse público, mediante a análise dos aspectos técnicos, operacionais e econômicos relacionados à demanda.

A elaboração do presente encontra fundamento na Lei Federal nº 14.133, de 1º de abril de 2021, que estabelece o planejamento como princípio e diretriz das contratações públicas e disciplina a fase preparatória dos processos de contratação, bem como na Instrução Normativa SEGES nº 58, de 8 de agosto de 2022, que dispõe sobre a elaboração dos Estudos Técnicos Preliminares para a contratação de bens e serviços no âmbito da Administração Pública.

No âmbito do Poder Legislativo Municipal, a elaboração deste estudo observa, ainda, as disposições da Portaria nº 215/2024, que regulamenta a aplicação da Lei Federal nº 14.133/2021 no âmbito da Câmara Municipal de Cachoeiro de Itapemirim/ES, sem prejuízo das demais normas legais, regulamentares e atos administrativos aplicáveis à matéria.

Nesse contexto, o ETP constitui importante instrumento de planejamento, permitindo que a Administração examine de forma estruturada a situação que originou a demanda, identifique suas necessidades, avalie as alternativas disponíveis, estabeleça os requisitos necessários ao atendimento do objeto, dimensione a solução pretendida, analise os aspectos econômicos envolvidos e verifique a viabilidade da contratação.

1. DESCRIÇÃO DA NECESSIDADE

O presente Estudo Técnico Preliminar (ETP) tem por finalidade identificar e analisar a necessidade administrativa da Câmara Municipal de Cachoeiro de Itapemirim – CMCI relacionada à **proteção do seu ambiente computacional contra ameaças cibernéticas**, bem como avaliar as alternativas disponíveis no mercado capazes de atender à demanda de forma adequada, eficiente e compatível com as necessidades institucionais.

A Câmara Municipal utiliza recursos de tecnologia da informação de forma contínua para o desenvolvimento de suas atividades administrativas e legislativas, incluindo computadores, notebooks,

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

servidores, sistemas informatizados, redes de comunicação, armazenamento e processamento de dados, correio eletrônico e demais recursos tecnológicos necessários ao funcionamento de seus setores.

A utilização intensiva desses recursos expõe o ambiente tecnológico institucional a diferentes tipos de ameaças cibernéticas, tais como vírus, malwares, ransomware, spyware, phishing, códigos maliciosos, exploração de vulnerabilidades, acessos indevidos e outras formas de ataques capazes de comprometer a segurança dos equipamentos, sistemas e informações.

A ocorrência de incidentes dessa natureza pode ocasionar indisponibilidade ou interrupção dos recursos tecnológicos, perda, alteração ou comprometimento de dados, propagação de códigos maliciosos na rede, redução da produtividade dos servidores e prejuízos à continuidade das atividades administrativas e legislativas desenvolvidas pela Câmara Municipal.

Diante desse cenário, torna-se necessária a adoção de mecanismos de proteção capazes de atuar de forma preventiva e contínua na identificação, bloqueio e tratamento de ameaças, proporcionando maior visibilidade sobre os equipamentos protegidos e permitindo o gerenciamento adequado das políticas de segurança do ambiente computacional.

Nesse contexto, a demanda consiste na disponibilização de solução corporativa de segurança para proteção dos endpoints e demais ativos tecnológicos abrangidos pela contratação, contemplando mecanismos atualizados de prevenção e detecção de ameaças, gerenciamento centralizado, atualização contínua e recursos que possibilitem o acompanhamento dos eventos de segurança e a adoção de medidas de resposta quando necessárias.

A solução a ser contratada deverá, ainda, ser compatível com o ambiente tecnológico existente na CMCI e possibilitar sua administração de maneira centralizada pela área responsável pela Tecnologia da Informação, de modo a contribuir para a padronização das políticas de segurança, o acompanhamento do estado de proteção dos dispositivos e a identificação tempestiva de eventuais ocorrências.

A necessidade também decorre da constante evolução das ameaças cibernéticas e da necessidade de manutenção de mecanismos de proteção devidamente atualizados durante todo o período de utilização da solução. Dessa forma, a contratação deverá assegurar a continuidade da proteção dos equipamentos abrangidos, evitando a exposição do ambiente institucional decorrente da utilização de ferramentas desatualizadas, insuficientes ou sem suporte.

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

2. PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL

A presente contratação deverá observar as disposições e diretrizes estabelecidas no Plano de Contratações Anual – PCA da Câmara Municipal de Cachoeiro de Itapemirim – CMCI, quando aplicável.

Caso a contratação não esteja contemplada no Plano de Contratações Anual vigente, sua realização deverá ser precedida da devida justificativa e das providências administrativas necessárias à sua inclusão ou adequação no planejamento institucional, observando-se a disponibilidade orçamentária e financeira, bem como as disposições da Lei Federal nº 14.133/2021 e da Lei Complementar nº 101/2000 – Lei de Responsabilidade Fiscal.

A contratação encontra-se alinhada às necessidades institucionais relacionadas à manutenção e ao aprimoramento da infraestrutura tecnológica da CMCI, à continuidade das atividades administrativas e legislativas e ao fortalecimento da segurança da informação, especialmente diante da necessidade de assegurar mecanismos adequados de proteção aos equipamentos e recursos tecnológicos utilizados pela Câmara Municipal.

3. REQUISITOS DA CONTRATAÇÃO

Para o adequado atendimento da necessidade identificada, a futura contratação deverá contemplar requisitos capazes de assegurar a disponibilização de solução de proteção e segurança para os equipamentos e recursos tecnológicos abrangidos, observadas as características do ambiente computacional da Câmara Municipal de Cachoeiro de Itapemirim – CMCI.

Os requisitos estabelecidos neste Estudo Técnico Preliminar têm caráter mínimo e deverão ser posteriormente detalhados e consolidados no Termo de Referência, após a conclusão das demais etapas de planejamento da contratação, especialmente quanto ao levantamento do quantitativo de dispositivos, compatibilidade tecnológica, funcionalidades necessárias, modelo de licenciamento e demais condições de execução.

Requisitos legais e normativos

A contratação deverá observar, no que couber, as disposições da legislação e regulamentação aplicáveis, especialmente:

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

- **Lei Federal nº 14.133, de 1º de abril de 2021**, que estabelece normas gerais de licitação e contratação para a Administração Pública;
- **Lei Complementar nº 123, de 14 de dezembro de 2006**, e suas alterações, no que se refere ao tratamento favorecido às Microempresas e Empresas de Pequeno Porte;
- **Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)**, quando houver tratamento de dados pessoais no âmbito da solução;
- **Lei Federal nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação**, no que couber;
- **Lei Federal nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet**, quando aplicável;
- **Portaria nº 215/2024**, que regulamenta a aplicação da Lei Federal nº 14.133/2021 no âmbito da Câmara Municipal de Cachoeiro de Itapemirim/ES;
- demais normas, regulamentos, atos administrativos e procedimentos internos da CMCI aplicáveis à contratação, à segurança da informação e à proteção de dados.

Requisitos de habilitação

A futura contratada deverá atender aos requisitos de habilitação jurídica, fiscal, social, trabalhista e econômico-financeira estabelecidos na legislação aplicável e no instrumento convocatório.

A documentação de habilitação deverá ser compatível com a natureza, o objeto e o vulto da contratação, observando-se os princípios da razoabilidade, proporcionalidade e ampliação da competitividade.

Os requisitos específicos de habilitação e eventual necessidade de comprovação de qualificação técnica deverão ser definidos no Termo de Referência e no instrumento convocatório, mediante justificativa compatível com as características efetivas da contratação.

Requisitos de qualificação técnica

Considerando a natureza da solução pretendida e sua relevância para a proteção do ambiente tecnológico institucional, deverá ser avaliada a necessidade de comprovação de capacidade técnica compatível com o objeto.

Quando exigida, a comprovação poderá ocorrer mediante apresentação de atestado(s) de capacidade técnica emitido(s) por pessoa jurídica de direito público ou privado, que demonstre(m) experiência anterior na prestação de serviços ou fornecimento de solução de natureza compatível com o objeto da contratação.

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

Eventuais quantitativos mínimos, níveis de similaridade, forma de comprovação e demais exigências deverão ser estabelecidos somente após a conclusão do levantamento da demanda e da análise de mercado, evitando-se requisitos desnecessários ou potencialmente restritivos à competitividade.

Requisitos técnicos e funcionais da solução

A solução a ser contratada deverá contemplar, no mínimo, recursos destinados à proteção dos equipamentos abrangidos contra ameaças cibernéticas, devendo ser compatível com o ambiente tecnológico da CMCI.

Entre os requisitos a serem considerados, destacam-se:

- proteção contra vírus, malware, spyware, trojans, worms e outros códigos maliciosos;
- mecanismos de proteção contra ransomware e outras ameaças que possam comprometer ou indisponibilizar dados;
- proteção em tempo real;
- atualização automática e contínua dos mecanismos de proteção;
- mecanismos de detecção de ameaças por análise comportamental e/ou heurística;
- capacidade de identificação de ameaças conhecidas e desconhecidas, conforme os recursos disponibilizados pela solução;
- recursos de EDR – Endpoint Detection and Response, caso confirmada sua necessidade após a análise das alternativas de mercado;
- gerenciamento centralizado dos dispositivos protegidos;
- disponibilização de console de gerenciamento, preferencialmente acessível por interface web;
- possibilidade de configuração e aplicação centralizada de políticas de segurança;
- geração de alertas, registros e relatórios relacionados ao estado de proteção e aos eventos de segurança;
- possibilidade de identificação de dispositivos com falhas, ameaças detectadas, ausência de atualização ou outras situações que demandem intervenção;
- mecanismos de resposta e contenção de incidentes, incluindo, quando disponibilizado pela solução, isolamento de equipamento comprometido;
- compatibilidade com os sistemas operacionais e demais características do ambiente tecnológico da CMCI;

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

- baixo impacto sobre o desempenho dos equipamentos protegidos, dentro das características técnicas da solução;
- disponibilização de documentação técnica suficiente para instalação, configuração, administração e utilização da solução.

Os requisitos técnicos detalhados, incluindo sistemas operacionais abrangidos, quantidade de dispositivos, funcionalidades obrigatórias, características do console de gerenciamento, políticas de atualização, recursos de EDR, mecanismos de resposta e demais especificações, deverão ser definidos no Termo de Referência após a conclusão da análise das alternativas disponíveis no mercado.

Requisitos de licenciamento

A solução deverá ser disponibilizada mediante licenciamento regular e legítimo, assegurando à Câmara Municipal o direito de utilização dos recursos contratados durante todo o período de vigência.

O licenciamento deverá contemplar as funcionalidades necessárias ao atendimento do objeto, bem como as respectivas atualizações e demais recursos que sejam indispensáveis ao funcionamento regular da solução, conforme o modelo comercial adotado pelo fabricante.

Não serão aceitas versões de avaliação, gratuitas, expiradas ou que não assegurem à Administração o direito regular de utilização durante o período contratado.

A modalidade de licenciamento, quantidade de licenças/subscrições, período de vigência e demais condições deverão ser definidas após o dimensionamento da demanda e a análise das soluções disponíveis no mercado.

Requisitos de atualização e manutenção da proteção

Durante toda a vigência contratual, a solução deverá permanecer em condições regulares de utilização, contemplando, conforme as características do produto contratado:

- atualização dos mecanismos de detecção e proteção;
- correções e atualizações necessárias ao funcionamento da solução;
- manutenção da compatibilidade com as versões suportadas dos sistemas operacionais;
- disponibilização das atualizações de segurança disponibilizadas pelo fabricante;
- manutenção do direito de utilização das funcionalidades contratadas.

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

A atualização contínua é requisito essencial, considerando a constante evolução das ameaças cibernéticas e a necessidade de que os mecanismos de proteção permaneçam atualizados durante toda a vigência da contratação.

Requisitos de suporte técnico

A solução deverá contar com suporte técnico adequado à sua utilização e administração pela CMCI, contemplando, no mínimo:

- canais formais para abertura e acompanhamento de solicitações;
- atendimento para esclarecimento de dúvidas e resolução de problemas relacionados à solução;
- suporte à instalação, configuração e utilização, quando previsto no modelo de contratação;
- orientação para tratamento de eventos ou incidentes relacionados à solução;
- disponibilização de documentação e orientações técnicas necessárias à administração do ambiente.

A necessidade de atendimento em regime **24 horas por dia, 7 dias por semana (24x7)**, bem como os respectivos níveis de serviço – SLA, deverá ser avaliada no decorrer do planejamento, considerando a criticidade do ambiente protegido e as alternativas disponíveis no mercado.

Os prazos de atendimento e solução, quando aplicáveis, serão estabelecidos no Termo de Referência, de acordo com os níveis de criticidade definidos pela Administração.

Requisitos de segurança da informação e proteção de dados

A solução e sua execução deverão observar as boas práticas aplicáveis à segurança da informação, bem como a legislação pertinente à proteção de dados pessoais.

Quando houver tratamento de dados pessoais, deverão ser observadas as disposições da Lei Federal nº 13.709/2018 – LGPD, especialmente quanto à adoção de medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados e situações acidentais ou ilícitas.

A solução deverá, ainda, disponibilizar mecanismos adequados de controle de acesso, registro de eventos e proteção das informações administradas pela ferramenta, quando compatíveis com suas características técnicas.

Eventuais requisitos adicionais relacionados a logs, auditoria, retenção de registros, integração com outras ferramentas de segurança e demais mecanismos de proteção deverão ser definidos no Termo de Referência, conforme a necessidade efetivamente identificada pela CMCI.

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

Requisitos de implantação e transferência de conhecimento

Caso a solução escolhida demande instalação, configuração, migração ou parametrização, a contratada deverá prestar o suporte necessário para sua adequada implantação no ambiente da CMCI.

Deverá ser avaliada, ainda, a necessidade de treinamento ou orientação técnica aos servidores responsáveis pela administração da solução, de forma a possibilitar sua utilização, configuração, acompanhamento e gerenciamento de maneira adequada.

Amostras e prova de conceito

Não se prevê, neste momento, a necessidade de apresentação de amostras físicas, considerando tratar-se de solução de software.

A comprovação do atendimento aos requisitos técnicos poderá ser realizada mediante análise da documentação oficial do fabricante, especificações técnicas, manuais, datasheets, declarações e demais documentos pertinentes.

A necessidade de realização de prova de conceito (PoC) deverá ser avaliada durante a elaboração do Termo de Referência, caso a complexidade da solução ou a necessidade de comprovação prática das funcionalidades justifique sua adoção.

Subcontratação

A possibilidade de subcontratação deverá ser definida no instrumento convocatório e no contrato, considerando a natureza da solução e o modelo de fornecimento adotado pelo fabricante.

A eventual participação de terceiros em atividades acessórias ou relacionadas à infraestrutura necessária ao funcionamento da solução não poderá afastar a responsabilidade integral da contratada perante a Administração pelo cumprimento das obrigações assumidas.

Microempresas e Empresas de Pequeno Porte

Deverão ser observados os benefícios e o tratamento favorecido assegurados às Microempresas – ME e Empresas de Pequeno Porte – EPP, nos termos da Lei Complementar nº 123/2006 e da legislação aplicável às contratações públicas.

A definição da forma de aplicação desses benefícios deverá considerar o valor estimado da contratação, a natureza do objeto e as demais condições estabelecidas na legislação e na regulamentação aplicáveis.

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

Vigência e continuidade da solução

Considerando que a proteção do ambiente computacional constitui necessidade de caráter contínuo, a contratação deverá assegurar a manutenção da proteção dos dispositivos abrangidos durante todo o período estabelecido pela Administração.

O período de vigência, a modalidade de licenciamento e eventual possibilidade de prorrogação deverão ser definidos observadas as disposições da Lei Federal nº 14.133/2021 e a natureza jurídica do objeto.

4. ESTIMATIVA DAS QUANTIDADES

A estimativa do quantitativo necessário para a contratação foi estabelecida de forma preliminar a partir da documentação técnica disponibilizada à Câmara Municipal de Cachoeiro de Itapemirim, pela empresa responsável pelo suporte à infraestrutura de tecnologia da informação, no qual foi indicada a necessidade de **140 (cento e quarenta) licenças** de solução de antivírus corporativo, destinadas à proteção dos equipamentos que compõem o ambiente tecnológico da CMCI.

Considerando que a solução a ser contratada deverá contemplar a proteção dos equipamentos institucionais abrangidos pela contratação, adota-se, nesta etapa de planejamento, o quantitativo preliminar de **140 (cento e quarenta) licenças**, conforme demonstrado a seguir:

Item	Descrição	Unidade de medida	Quantidade estimada
01	Licenças de solução corporativa de proteção de endpoints, contemplando funcionalidades de EDR – Endpoint Detection and Response	Licença	**140**

O quantitativo acima corresponde, portanto, à previsão inicial para dimensionamento da contratação, considerando-se a necessidade de disponibilização da solução de segurança aos equipamentos abrangidos pelo ambiente tecnológico da Câmara.

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

5. LEVANTAMENTO DE MERCADO

Considerando a necessidade identificada no presente Estudo Técnico Preliminar, foi realizado levantamento das soluções disponíveis no mercado destinadas à proteção de equipamentos de tecnologia da informação contra ameaças cibernéticas, considerando a evolução das ferramentas de segurança de endpoints e os diferentes níveis de proteção, monitoramento e resposta disponibilizados pelos fabricantes.

A análise das alternativas de mercado permitiu identificar, de forma geral, as seguintes possibilidades:

I. **Antivírus convencional:** solução destinada principalmente à prevenção e detecção de códigos maliciosos, utilizando mecanismos como assinaturas, análise heurística e proteção em tempo real. Embora atenda à necessidade básica de proteção contra malware, apresenta recursos mais limitados para investigação de incidentes, análise comportamental e resposta centralizada a ameaças.

II. **Plataforma corporativa de proteção de endpoints – EPP:** solução voltada ao gerenciamento e à proteção centralizada de estações de trabalho e servidores, normalmente incorporando mecanismos de proteção em tempo real, análise comportamental, proteção contra ransomware, controle de dispositivos, atualizações automáticas, políticas de segurança, alertas e relatórios.

III. **Plataforma de proteção de endpoints com recursos de EDR** – Endpoint Detection and Response: além das funcionalidades de proteção preventiva próprias de uma solução EPP, incorpora mecanismos destinados à identificação de comportamentos suspeitos, análise de eventos, investigação de incidentes, correlação de informações e adoção de medidas de resposta e contenção nos equipamentos protegidos.

IV. **Soluções XDR – Extended Detection and Response:** ampliam a capacidade de detecção e correlação de eventos para além dos endpoints, podendo integrar informações provenientes de diferentes camadas do ambiente tecnológico, tais como servidores, correio eletrônico, serviços em nuvem, rede e outras fontes de telemetria. Embora representem uma evolução das plataformas de segurança, sua utilização pressupõe um ambiente tecnológico e uma estrutura de segurança mais abrangentes, cuja necessidade específica não foi identificada no presente estudo.

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

V. **Serviços MDR – Managed Detection and Response:** consistem na contratação de serviço especializado para monitoramento e resposta a incidentes de segurança, normalmente envolvendo equipe especializada do fornecedor atuando de forma contínua sobre os eventos de segurança da organização. Trata-se de modelo que extrapola o simples fornecimento de licenças de software e implica a contratação de serviço especializado de monitoramento e resposta.

Análise das alternativas

As alternativas identificadas foram analisadas considerando sua capacidade de atender à necessidade institucional, o nível de proteção oferecido, a capacidade de gerenciamento centralizado, os mecanismos de detecção de ameaças, a possibilidade de resposta a incidentes, a compatibilidade com o ambiente tecnológico existente, a complexidade de implantação e administração e os custos associados à contratação.

A solução de **antivírus convencional,** embora represente alternativa de menor complexidade, possui atuação predominantemente preventiva e apresenta menor capacidade de identificação e investigação de comportamentos suspeitos quando comparada às plataformas corporativas mais modernas.

A adoção de uma **plataforma corporativa EPP** representa evolução em relação ao antivírus convencional, especialmente pela possibilidade de administração centralizada, aplicação de políticas, acompanhamento dos equipamentos protegidos, geração de alertas e utilização de mecanismos adicionais de proteção.

Por sua vez, a **plataforma EPP com funcionalidades de EDR** agrega às capacidades de prevenção e proteção características voltadas à detecção, investigação e resposta a ameaças, permitindo maior visibilidade sobre os eventos ocorridos nos endpoints e possibilitando ações de contenção e resposta de acordo com os recursos disponibilizados pelo fabricante.

Também foi identificada, em contratação realizada por outro órgão público, a utilização de solução de antivírus com funcionalidade de EDR para estações de trabalho, servidores e dispositivos móveis, com gerenciamento centralizado, instalação, suporte técnico e atualizações contínuas, evidenciando que esse modelo de solução constitui alternativa disponível e utilizada no mercado para proteção corporativa de endpoints.

As soluções **XDR** e **MDR**, embora tecnicamente disponíveis, apresentam abrangência e complexidade superiores à necessidade atualmente caracterizada neste estudo. Sua adoção exigiria a demonstração de necessidades adicionais relacionadas à integração de múltiplas camadas de segurança, monitoramento

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

especializado ou operação contínua de um serviço de resposta, não sendo identificados, até o presente momento, elementos suficientes que justifiquem a ampliação do objeto para esses modelos.

Solução definida para a contratação

Diante das alternativas analisadas, **define-se como solução a ser considerada para a presente CONTRATAÇÃO A AQUISIÇÃO DE LICENÇAS DE SOLUÇÃO CORPORATIVA DE PROTEÇÃO DE ENDPOINTS (EPP), CONTEMPLANDO FUNCIONALIDADES DE EDR – ENDPOINT DETECTION AND RESPONSE, destinada à proteção dos equipamentos de tecnologia da informação da Câmara Municipal de Cachoeiro de Itapemirim.**

A escolha dessa alternativa decorre da necessidade de superar a proteção exclusivamente convencional, proporcionando à Administração uma plataforma corporativa capaz não apenas de prevenir e bloquear ameaças, mas também de ampliar a visibilidade sobre eventos de segurança e possibilitar resposta mais adequada diante de incidentes.

6. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Para fins de análise preliminar da viabilidade da contratação, foi utilizada como referência contratação anteriormente realizada pela própria Câmara Municipal de Cachoeiro de Itapemirim, no exercício de 2025, referente à renovação de licenças da solução de antivírus da Trend Micro, com atualização do licenciamento para o Trend Vision One – Endpoint Security (Essentials), incluindo as atualizações de versão, pelo período de 12 (doze) meses.

Conforme consta da Autorização de Fornecimento nº 000125/2025, vinculada ao Processo de Contratação nº 18840/2025, a contratação da solução foi realizada pelo valor total de R$ 36.099,00 (trinta e seis mil e noventa e nove reais), para vigência de 12 (doze) meses.

Considerando-se, exclusivamente para fins de projeção preliminar, a manutenção do referido valor anual durante o período de 36 (trinta e seis) meses, obtém-se a seguinte estimativa:

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

Descrição	Referência anual	Período considerado	Estimativa preliminar
Solução corporativa de proteção de endpoints	R$ 36.099,00	36 meses	**R$ 108.297,00**

Assim, para fins deste Estudo Técnico Preliminar, estima-se preliminarmente o valor de **R$ 108.297,00 (cento e oito mil, duzentos e noventa e sete reais)** para a contratação pelo período de 36 (trinta e seis) meses.

Ressalta-se que o valor acima possui **caráter exclusivamente preliminar e referencial**, destinando-se à análise da viabilidade econômica da solução durante a fase de planejamento da contratação.

A estimativa definitiva do valor da contratação será realizada em etapa posterior, por ocasião da elaboração do Termo de Referência, mediante pesquisa de preços compatível com as características definitivas do objeto, considerando-se, conforme aplicável, contratações públicas similares, preços praticados no mercado e demais fontes.

7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução considerada para atendimento da necessidade consiste na contratação de empresa especializada para fornecimento de licenças de software de proteção corporativa de endpoints, contemplando recursos de antivírus e mecanismos avançados de detecção e resposta a ameaças, incluindo funcionalidade de EDR – Endpoint Detection and Response, pelo período 36 meses, abrangendo as estações de trabalho e os servidores que integram o ambiente tecnológico da Câmara Municipal de Cachoeiro de Itapemirim.

A solução deverá proporcionar proteção centralizada dos ativos computacionais, permitindo o gerenciamento, monitoramento, aplicação de políticas de segurança, atualização, identificação e tratamento de eventos de segurança a partir de console de administração unificada.

Proteção dos equipamentos

a) Prover segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado.

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

b) Possuir console central única de gerenciamento. As configurações do Antivírus, AntiSpyware, Firewall, Detecção de intrusão controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console;

c) O Produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;

d) O produto deverá possuir no mínimo os seguintes módulos:

e) Console de Gerenciamento fornecendo funcionalidades de gestão;

f) Módulos para estações físicas, laptops e servidores;

g) Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;

h) Utilizar o conceito de heurística;

i) Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);

j) Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware;

k) Oferecer inventário de softwares;

l) Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;

m) Oferecer proteção por base de assinaturas;

Console de gerenciamento

A solução deverá disponibilizar console de gerenciamento destinada à administração centralizada do ambiente de segurança, podendo ser disponibilizada como appliance virtual, executável para instalação em servidor Windows ou mediante console de gerenciamento em nuvem.

A console deverá contemplar, conforme as características previstas na solução de referência:

a) Instalação e configuração

b) Deve ser fornecido como um appliance virtual ou executável para instalação em servidores Windows ou Console com Gerenciamento na nuvem (Cloud).

c) Deverá suportar no mínimo os seguintes Hypervisors: VMWare vSphere, Citrix XenServer; XenDesktop, VDI-ina-Box;

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

d) Microsoft Hyper-V, Red hat Enterprise Virtualization, Kernel-based Virtual Machine ou KVM, Oracle VM;

e) Deverá ser fornecido com base de dados embutido na Console em Nuvem, sem a necessidade de baixar para máquina do administrador da Console;

f) Permitir instalação remota via console WEB de gerenciamento para ambientes virtual VMWare ou Citrix;

g) O mecanismo de varredura deverá estar disponível para download separadamente;

h) A solução deverá permitir a inclusão de um modulo de balanceamento para casos em vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance entre outras);

i) Deve ser totalmente em português.

Características gerais

A solução deverá possibilitar administração centralizada dos recursos de segurança, contemplando:

a) Arquitetura simples de atualização, com botão único para acesso a todas as funções e serviços serem atualizados;

b) Permitir que o administrador escolha qual o pacote será atualizado;

c) As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador;

d) No mínimo enviar notificações: Problemas com licenças, Alertas de Surto de vírus, Máquinas desatualizadas, Eventos de antimalware,

e) Painel para Monitoramento baseado em "portlets" configuráveis com no mínimo as seguintes especificações: Nome; Tipo de relatório; Alvo do relatório;

f) Deverá disponibilizar "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;

g) Inventário da Rede

h) Possuir no mínimo as integrações abaixo: Múltiplos domínios do Active Directory, Múltiplos VMWare vCenters, Múltiplos Citrix Xen Servers;

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

i) Possuir a possibilidade de definição de sincronização com o Active Directory em horas;

j) Deverá ser compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;

k) Descoberta de rede para máquinas em grupo de trabalho;

l) Possuir busca em tempo real pelo menos com os seguintes filtros: Nome, Sistema Operacional e Endereço IP;

m) Possibilitar a instalação remota e desinstalação remota do antivírus;

n) Possibilitar a configuração de pacotes de instalação do produto de antivírus;

o) Possuir tarefas remotas e configuráveis de Scan;

p) Possuir tarefa de reinicialização remota de estação ou servidor;

q) Assinar políticas para no mínimo os níveis: Computador, Máquina Virtual ou Possuir a propriedade detalhada de objetos gerenciados para: Nome, IP, Sistema Operacional, Grupo, Política Assinada, último status de malware;

Políticas

a) Modelo único para todos os equipamentos, seja físico ou virtual;

b) Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;

c) Deverá configurar as funcionalidades como escaneamento do Antivírus, firewall de duas vias de detecção de intrusão, controle de acesso a rede, controle de aplicação, controle de acesso web, autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade;

Relatórios

a) Relatório para cada serviço de segurança;

b) Facilidade de usar e visualização simplificada;

c) Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;

d) Filtros de agendamento de relatórios;

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

e) Arquivo com todas as instâncias de relatório agendados;

f) Exportar o relatório nos formatos .pdf e/ou .csv;

g) Oferecer possibilidade de criar relatórios de maneira dinâmica no painel administrativo da solução.

h) Quarentena

i) Restauração remota, com configuração de localidade e deleção;

j) Criação e exclusão para arquivos restaurados;

Usuários

a) Administração baseada em regras;

b) Disponibilizar tipos de usuários pré-definidos como no mínimo: Administrador - Gerente dos componentes da solução, Administrador de rede - Gerente dos serviços de segurança;

c) Relatório - Monitora e cria relatórios;

d) Deverá ser possível customizar um tipo de usuário;

e) Deverá permitir a integração do usuário com o Active Directory para autenticação da console de gerenciamento;

f) Logs de utilização;

g) Registrar as ações do usuário na console de gerenciamento;

h) Detalhar cada ação do usuário;

i) Permitir busca complexa baseada em ações do usuário, intervalos de tempo;

Certificado de Segurança

a) Deverá prover o acesso via HTTPS;

b) Deverá permitir a importação de certificados digitais;

c) O gerenciamento e a comunicação com dispositivos móveis deve ser feito de forma segura utilizando certificados digitais;

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

Proteção Para Estações De Trabalho E Servidores Físicos

a) Deverá permitir a configuração do scan do antivírus do cliente como: Scan local, Scan Hibrido, Scan Central;

b) Deverá permitir a instalação customizada do antivírus com no mínimo: Instalar o antivírus sem o controle de acesso a internet; Instalar o antivírus sem o módulo de firewall;

c) Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 11, Windows 10 32 e 64Bits, Windows 7 32 e 64Bits.

d) Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: Windows Server 2025, Windows Server 2022, Windows Server 2019 Core, Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2.

e) Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux: Ubuntu 14.04 LTS ou superior, Red Hat Enterprise Linux / CentOS 6.0 ou superior, SUSE Linux Enterprise Server 11 SP4 ou superior, OpenSUSE Leap 42.x, Fedora 25 ou superior, Debian 8.0 ou superior, Oracle Linux 6.3 ou superior, Amazon Linux AMI 2016.09 ou superior;

Gerenciamento e Instalação Remota

a) Deverá permitir ao administrador customizar a instalação;

b) A instalação deverá ser possível executar com no mínimo das seguintes maneiras: Executar o pacote de antivírus diretamente na estação de trabalho, instalar remotamente, distribuído via console de gerência web;

c) Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;

d) A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações: Nome, IP, Sistema Operacional, Política Aplicada;

e) Através da console, o administrador poderá enviar uma política única para configurar o antivírus;

f) A console de gerenciamento deverá incluir sessão de log com as seguintes informações: Login, Edição, Criação, Log-out, ter a capacidade de criar um único pacote independente ser for para 32

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

bits ou 64 bits, deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;

g) O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário à distribuição em um agente separado;

Proteção Para Estações E Servidores Virtuais

a) Proteção de antivírus dedicado para ambientes virtuais;

b) Deverá ter a disponibilidade de ser integrado com o VMWare e oferecer a escaneamento sem instalar o produto na máquina virtual;

c) A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;

d) Deverá proteger em tempo real e agendado as máquinas virtuais Linux;

e) O produto deverá oferecer agente para virtualização dos seguintes produtos: Citrix Xen Server, Microsoft Hyper-V, Red Hat Virtualization, Oracle KVM, KVM;

Funções Gerais

a) Deverá ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;

b) Deverá reportar o estado atual das VMs no mínimo, protegida/desprotegida;

c) Requisitos Mínimos suportados pelo Sistema.

d) Plataformas de Virtualização: VMware vSphere and vCenter Server: versão 6.5; version 6.7, incluindo update 1, update 2a e update 3; version 7.0, incluindo update 1, update 2, update 2b, update 2c e update 2d; version 8.0, incluindo update 1, update 2.VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x VMware Workstation 11.x, 10.x, 9.x, 8.0.6VMware Player 7.x, 6.x, 5.x Citrix Xen Hypervisor: 7.1 (with the XS71ECU2060 hotfix), 8.2.Citrix Virtual Apps e Desktops 7 1808, 7 1811, 7 1903, 7 1906 Citrix XenApp e XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR Citrix VDI-in-a-Box 5.x Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019,2022,2025 (incluindo Hyper-V Hypervisor) Red Hat Enterprise Virtualization 3.0 (incluindo KVM Hypervisor) Oracle VM 3.0 Oracle VM VirtualBox 5.2, 5.1 Nutanix Prism com AOS

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

5.6, 5.5, 5.20 LTS, 5.18 STS,5.15 LTS, 5.11, 5.10 (Enterprise Edition) Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 e 20190916.294 (Community Edition)

e) Sistemas Operacionais desktops (32 e 64 Bits): Windows 7, Windows 10, Windows 11

f) Sistemas Operacionais Servidores: Windows Server 2025, Windows Server 2022, Windows Server 2019 Core Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2, Ubuntu 14.04 LTS ou superior, Red Hat Enterprise Linux / CentOS 6.0 ou superior, SUSE Linux Enterprise Server 11 SP4 ou superior, OpenSUSE Leap 42.x, Fedora 25 ou superior, Debian 8.0 ou superior, Oracle Linux 6.3 ou superior, Amazon Linux AMI 2016.09 ou superior;

Componentes e Funcionalidade do Antivírus Geral

a) Deverá fazer scan em tempo real automático;

b) Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;

c) scaneamento de comportamento heurístico;

d) Deverá escanear em tempo real qualquer informação localizadas em mídias de armazenamento como:

e) CD/DVD, Discos Externos, Pen-Drivers, Deverá permitir a escolha e configuração de pastas a serem escaneada;

f) Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção: Baseada em Assinaturas, Baseada em Heurística, Baseada em monitoramento contínuo de processos;

g) Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL na Estações de trabalho;

h) O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas Search Advisor na Estações de trabalho;

i) Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser

j) instalado/desinstalado nas estações de trabalho;

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

k) O módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;

l) Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;

m) Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;

n) Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;

o) Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;

p) Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas;

Controle de Usuário

a) Deverá ter módulo de controle de usuário integrando com as seguintes características: Bloqueio de acesso à internet, Bloqueio de acesso a aplicações definidas pelo administrador;

Controle do Dispositivo

a) Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;

b) Através do módulo de controle de dispositivo deverá ser possível controlar: Bluetooth, CDROM/DVDROM, IEEE 1284.4, IEEE 1394, Windows Portable, Adaptadores de Rede, Adaptadores de rede Wireless, Discos Externos;

c) Deverá permitir regras de definição de bloqueio/desbloqueio;

d) Deverá permitir regras de exclusão;

Atualização

a) Após a atualização o administrador deverá ter a capacidade de adiar uma reinicialização;

b) Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;

c) Permitir atualizações de assinatura de hora em hora;

d) Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

e) Proteção para caixa de e-mail:

f) Fornecer proteção para ambiente Exchange

g) Oferecer tecnologia para proteção contra spam;

h) Oferecer análise comportamental e proteção para zero-day;

i) Oferecer proteção contra vírus e tentativas de phishing;

Criptografia

a) Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-premise com módulo de Criptografia presente na mesma Console do Antivirus.

b) Deverá utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault);

c) Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;

d) Deverá ser compatível com:

- macOS Sonoma (14.x)
- macOS Ventura (13.x)
- macOS Monterey (12.x)
- macOS Big Sur (11.x)

Proteção Avançada NGAV

a) Detectar e bloquear todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como eliminar malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware. Detectar e bloquear ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques sem arquivos e malware sofisticado, devendo ser detectados e bloqueados antes de serem executados.

b) Detectar e parar, bloquear e interromper malwares sem arquivos.

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

c) Parar os ataques com base em macros e scripts. Analisar scripts, como Powershell, WMI, intérpretes de Javascript, etc, bem como adicionar técnicas de analisador de linha de comando para interceptar e proteger scripts, enquanto alerta os administradores e bloqueia a execução de scripts no caso de executar comandos maliciosos.

d) Reparo e resposta automatizada a ameaças

e) Quando uma ameaça é detectada, a ferramenta deve neutralizá-la imediatamente por meio de ações que incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mal-intencionadas. Compartilhar as informações sobre ameaças em tempo real com a GPN, o serviço de inteligência contra ameaças baseadas na nuvem do fabricante, para impedir ataques semelhantes.

f) Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional.

g) Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente.

h) Deverá ter um nível de proteção na fase de pré-execução com modelos locais de aprendizado de máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas. Também deverá detectar técnicas de propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na web. Deverá permite que os administradores de segurança ajustem a proteção para combater os riscos.

Machine Learning

As técnicas de Machine Learning devem utilizar modelos e algoritmos extensamente treinados para prever e bloquear os ataques avançados.

As ferramentas de Machine Learning devem, se basear em características estáticas e dinâmicas, e se treinarem continuamente com bilhões de amostras de arquivos legítimos e maliciosas devendo melhorar significativamente a efetividade da detecção de malware e minimizar os falsos positivos. ações evasivas e conexões a centros de comando e controle.

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

Sandbox

Sandbox integrado nos terminais que deverá analisar arquivos suspeitos em profundidade, acionar ações destrutivas em um ambiente virtual isolado, hospedado pelo fabricante, analisando seu comportamento e informando sobre intenções maliciosas. O Sandbox deve ser integrado com o agente e encaminhar automaticamente os arquivos suspeitos para análise. Ao retornar uma análise com resultado "malicioso", o Sandbox deverá bloquear automaticamente o arquivo malicioso em sistemas em toda rede imediatamente. O recurso de envio automático deve permitir que os administradores de segurança da empresa escolham o modo de monitoramento ou bloqueio, o que impede o acesso a um arquivo até que um resultado seja emitido. Os administradores também podem enviar arquivos manualmente para análise. As informações forenses devem fornecem um contexto claro das ameaças e ajudar a entender o comportamento delas.

Antiexploit Avançado

Deverá conter antiexploit avançado para prevenção de exploração e proteção a memória e aplicativos vulneráveis, como navegadores, leitores de documentos, arquivos multimídia e tempo de execução (ou seja:Flash ou Java). Os ecanismos avançados devem observar a rotina de acesso na memória para detectar e bloquear técnicas de exploração, como verificação de chamadas de API, pivotamento de pilha, ROP (returnoriented programming), etc.

Inspetor de processo

O Inspetor de Processos deverá operar em um modo de confiança zero, monitorando continuamente todos os processos em execução no sistema operacional. Deverá procurar atividades suspeitas ou comportamentos anormais de processos, como tentativas de ocultar o tipo de processo, executar código no espaço de outro processo (seqüestro de memória do processo para escalonamento de privilégios), replicar, descartar arquivos, ocultar para processar aplicativos de listagem etc. Tomar as medidas de reparação adequadas, incluindo o encerramento do processo e a reversão das alterações efetuadas. Deverá detectar de malwares desconhecidos, avançados e ataques sem arquivos, incluindo ransomware.

Detecção e Resposta - EDR

Deverá realizar a correlação entre terminais, conhecida como EDR, levando a detecção de ameaças bem como aplicar funcionalidades de XEDR para detectar ataques avançados em vários terminais em infraestruturas híbridas (estações de trabalho ou servidores executando vários sistemas operativos)

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

Deverá analisar continuamente os riscos usando centenas de fatores para descobrir e priorizar os riscos de configuração para todos os seus terminais, permitindo ações automáticas de fortalecimento. Identificar ações e comportamentos dos usuários que representam um risco de segurança para a organização, como o uso de páginas web não criptografadas para fazer login em sites, gerenciamento de senhas inadequado, uso de USBs comprometidos, infecções recorrentes, etc.

Posicionamento de mercado

O fabricante/desenvolvedor da solução de proteção de endpoints, deverá estar presente no quadrante mágico do Gartner mais recente, de forma que possa ser adquirida uma solução mais confiável, madura e robustas do mercado, contando com a prestação de serviços qualificados, potencializando o sucesso desta contratação. Vale ressaltar que a utilização do quadrante mágico do Gartner, é prática comum entre as contratações públicas de TIC e que a adoção deste requisito, não fere os princípios da isonomia e da competitividade, visto que a maioria dos principais fabricantes/desenvolvedores constam no último quadrante mágico em vigência, no momento da escrita deste Termo.

Sendo assim, o fabricante/desenvolvedor desta solução deverá constar no quadrante mágico para EPP (plataformas de proteção de endpoint) do Gartner mais recente, em qualquer categoria, seja de líderes, visionários, competidores de nicho ou desafiadores.

8. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Nos termos da Lei Federal nº 14.133/2021, foi analisada a possibilidade de parcelamento do objeto, considerando a natureza, as características e a forma de funcionamento da solução pretendida, concluindo-se que **não se mostra recomendável o parcelamento da contratação**.

A contratação de uma solução integrada possibilita a **centralização da gestão dos ativos protegidos**, a padronização dos mecanismos de segurança, a uniformidade das atualizações e políticas aplicadas e a concentração do suporte técnico em um único fornecedor, facilitando a fiscalização e o acompanhamento da execução contratual.

Dessa forma, considerando a interdependência funcional entre os componentes que integram a solução, a contratação em **item/lote único** mostra-se tecnicamente adequada ao atendimento da necessidade

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

identificada, favorecendo a padronização, a eficiência operacional, a simplificação da gestão contratual e a adequada administração da segurança dos equipamentos abrangidos pela contratação.

9. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

Com a contratação da solução, pretende-se alcançar os seguintes resultados:

a) Fortalecimento da segurança da informação

- ampliar a proteção dos equipamentos institucionais contra vírus, malwares, ransomware e outras ameaças cibernéticas;
- reduzir a exposição dos ativos de tecnologia da informação a incidentes de segurança;
- manter mecanismos de proteção atualizados, acompanhando a evolução das ameaças cibernéticas;
- possibilitar maior controle sobre os dispositivos abrangidos pela solução de segurança.

b) Proteção e continuidade das atividades institucionais

- contribuir para a redução de incidentes que possam ocasionar indisponibilidade ou comprometimento dos equipamentos e sistemas utilizados pela Câmara;
- reduzir os riscos de interrupções das atividades administrativas decorrentes de incidentes de segurança da informação;
- contribuir para a preservação da disponibilidade dos recursos tecnológicos necessários ao funcionamento institucional.

c) Eficiência na gestão da segurança da informação

- proporcionar maior eficiência na administração da proteção dos equipamentos institucionais;
- possibilitar, conforme as funcionalidades disponibilizadas pela solução contratada, o gerenciamento centralizado, o acompanhamento dos eventos de segurança e a aplicação de políticas de proteção;
- facilitar a identificação e o tratamento de ocorrências de segurança, reduzindo a necessidade de intervenções manuais e descentralizadas.

d) Proteção dos dados e do patrimônio informacional

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

- reduzir os riscos de perda, alteração, indisponibilidade ou comprometimento de informações institucionais decorrentes de códigos maliciosos e outras ameaças;
- contribuir para a preservação da integridade, disponibilidade e confidencialidade das informações tratadas no ambiente computacional da Câmara;
- proteger os investimentos realizados pela Administração em equipamentos, sistemas e infraestrutura de tecnologia da informação.

e) Redução de riscos e de custos decorrentes de incidentes

A adoção de mecanismo adequado de proteção dos endpoints deverá contribuir para a prevenção e mitigação de incidentes que possam gerar custos adicionais à Administração, tais como recuperação de equipamentos, restauração de sistemas, recuperação de dados, indisponibilidade de recursos tecnológicos e eventual necessidade de contratação emergencial de serviços especializados.

f) Conformidade e governança

- contribuir para o atendimento das normas e diretrizes aplicáveis à segurança da informação e à proteção de dados no âmbito da Administração Pública;
- contribuir para o cumprimento das disposições pertinentes da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), especialmente quanto à adoção de medidas técnicas e administrativas destinadas à proteção das informações;
- fortalecer as práticas de governança e gestão de segurança da informação no ambiente institucional.

10. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO

Para garantir a adequada execução da futura contratação, a Administração deverá adotar, previamente e durante a execução contratual, as providências necessárias à implantação, utilização e fiscalização da solução, observadas as características da solução que vier a ser contratada.

Planejamento da implantação

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

O setor de Tecnologia da Informação da CMCI deverá realizar o planejamento da implantação da solução, contemplando, conforme aplicável:

- levantamento e validação dos equipamentos que serão abrangidos pela contratação;
- conferência do ambiente computacional existente;
- verificação da compatibilidade da solução com os sistemas operacionais e demais recursos tecnológicos utilizados pela Câmara;
- definição do cronograma e das etapas necessárias à implantação;
- identificação de eventuais interferências com soluções de segurança atualmente instaladas.

Designação da equipe de fiscalização

A Administração deverá designar os servidores responsáveis pelo acompanhamento e fiscalização da futura contratação, nos termos do art. 117 da Lei Federal nº 14.133/2021 e demais normas aplicáveis.

Compete à equipe de fiscalização, conforme as atribuições estabelecidas pela Administração:

- acompanhar a execução contratual;
- verificar a conformidade das licenças e dos serviços fornecidos com as condições estabelecidas no instrumento contratual;
- acompanhar a disponibilização e a manutenção da solução durante a vigência contratual;
- registrar ocorrências relacionadas à execução do contrato;
- comunicar à autoridade competente eventuais irregularidades identificadas;
- subsidiar o atesto e o recebimento do objeto, conforme os procedimentos internos aplicáveis.

Preparação do ambiente tecnológico

Previamente à implantação da solução, o setor responsável deverá avaliar as condições do ambiente tecnológico da Câmara, adotando, quando necessárias e tecnicamente justificadas, medidas como:

- atualização dos sistemas operacionais e demais componentes relevantes;
- identificação e eventual remoção ou desativação de soluções de segurança incompatíveis;

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

- realização de procedimentos de segurança e preservação das configurações existentes, quando aplicável;
- atualização do inventário dos equipamentos abrangidos pela solução;
- verificação dos requisitos técnicos necessários ao funcionamento da solução contratada.

Gestão e acompanhamento contratual

Durante a vigência contratual, a Administração deverá acompanhar, entre outros aspectos pertinentes:

- a validade e a disponibilidade das licenças contratadas;
- a disponibilização das atualizações e mecanismos de proteção previstos na solução;
- o funcionamento e a aderência da solução às condições estabelecidas no contrato;
- os níveis e prazos de atendimento do suporte técnico, quando previstos;
- a ocorrência de falhas, indisponibilidades ou outros eventos que possam comprometer a execução contratual;
- o cumprimento das demais obrigações assumidas pela contratada.

11. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

No levantamento realizado para a elaboração deste Estudo Técnico Preliminar, não foram identificadas, até o momento, contratações correlatas ou interdependentes que sejam indispensáveis à execução do objeto pretendido.

12. IMPACTOS AMBIENTAIS

Por se tratar de contratação de solução de software, os impactos ambientais diretos são reduzidos.

Serão observadas, quando aplicáveis, boas práticas de sustentabilidade, especialmente:

- utilização de licenciamento e disponibilização eletrônica, reduzindo o uso de mídias físicas;
- redução de resíduos e deslocamentos técnicos, mediante suporte remoto, quando possível;

Praça Jerônimo Monteiro, 70, Centro
Cachoeiro de Itapemirim/ES
CEP: 29300-170
Contato: +55 28 3526-5622
e-mail: presidenciacmci@cachoeirodeitapemirim.es.leg.br

- contribuição para a preservação dos equipamentos por meio de proteção preventiva.

A contratada deverá observar a legislação ambiental aplicável, inclusive a Lei Federal nº 12.305/2010 – Política Nacional de Resíduos Sólidos, quando pertinente à execução contratual.

13. POSICIONAMENTO CONCLUSIVO SOBRE A VIABILIDADE DA CONTRATAÇÃO

Diante das análises realizadas, conclui-se que a contratação de solução corporativa de proteção dos ativos de tecnologia da informação é **tecnicamente e operacionalmente viável**, mostrando-se adequada ao atendimento da necessidade identificada pela Câmara Municipal de Cachoeiro de Itapemirim.

A solução deverá contribuir para o fortalecimento da segurança da informação, a proteção dos equipamentos e a continuidade das atividades institucionais.

Dessa forma, declara-se a **viabilidade da contratação**, recomendando-se o prosseguimento dos procedimentos necessários à elaboração do Termo de Referência e à realização da contratação, observadas a legislação aplicável e as conclusões da pesquisa de mercado.

Cachoeiro de Itapemirim, 18 de setembro de 2026

Mateus Rebonato Santos:08350798726

Assinado de forma digital por Mateus Rebonato Santos:08350798726
Dados: 2026.10.19 10:41:36 -03'00'

Mateus Rebonato Santos
Analista Prévio de Aquisições e Contratações