



# *Câmara Municipal de Carapicuíba*

Estado de São Paulo

## **ESTUDO TÉCNICO PRELIMINAR INTRODUÇÃO**

Estudo técnico preliminar para a manutenção da solução de segurança de endpoints ESET Protect Advanced, já consolidada em seu uso na Câmara Municipal de Carapicuíba, com vistas a instruir procedimento de contratação preferencialmente por dispensa de licitação, nos termos da Lei nº14.133/2021, a ser devidamente analisada e enquadrada pela assessoria jurídica.

### **1. DESCRIÇÃO DA NECESSIDADE**

A Câmara Municipal de Carapicuíba já utiliza a solução ESET Protect Advanced há aproximadamente 3 anos, com 80 licenças distribuídas entre estações de trabalho, notebooks e servidores devidamente protegidos.

Dessa solução, 75 licenças devem ser renovadas e 5 licenças ainda estão em uso, com validade até 24 de janeiro de 2028.

Opera com console centralizado de gerenciamento em nuvem para aplicação de políticas de segurança, monitoramento de incidentes, inventário de ativos e geração dos relatórios de auditoria de ameaças cibernéticas.

Depende da solução para mitigação dos seguintes riscos:

- Ransomware e outras ameaças que possam criptografar arquivos;
- Ameaças de dia zero (zero-day) e malware avançado;
- Vazamento de dados sensíveis e sigilosos decorrentes de perda, furto ou acesso não autorizado a dispositivos.
- Indisponibilidade de sistemas críticos que suportam todas as atividades legislativas e administrativas.

### **2. ÁREA REQUISITANTE**

<b>Área requisitante</b>	<b>Responsável</b>
Setor de TI	Milton Uemura

### **3. REQUISITOS DA CONTRATAÇÃO**

A contratação se refere a um serviço de natureza contínua e essencial, voltado à proteção de endpoints, estações de trabalho e servidores, bem como da gestão centralizada da segurança da informação, evitando assim:



# *Câmara Municipal de Carapicuíba*

Estado de São Paulo

- Interrupção da cobertura de antivírus por expiração de licenças;
- Fragmentação da segurança por uso simultâneo de múltiplas soluções heterogêneas;
- Aumento exponencial do risco de incidentes cibernéticos que afetem a integridade, confidencialidade e disponibilidade das informações armazenadas na Câmara Municipal;
- Prejuízos à imagem institucional, à transparência e à continuidade do serviço público legislativo.

## **Suporte Técnico**

O suporte técnico deverá contemplar a disponibilização de uma central de atendimento em horário comercial (das 09:00h às 18:00h) e em dias úteis (segunda a sexta-feira), por meio de registro de chamados por telefone ou sítio eletrônico oficial.

## **Treinamento**

As atividades de treinamento compreenderão a elaboração de quaisquer atividades técnicas relacionadas à utilização dos sistemas.

Isso inclui a compreensão das funções do software atribuídas à sua área de responsabilidade, conhecimento sobre as parametrizações a serem utilizadas, políticas de segurança a serem criadas, além do manejo das rotinas de segurança.

Após a capacitação, espera-se que cada servidor seja capaz de operar proficientemente o sistema designado a ele.

O futuro contratado será responsável por prover todos os recursos, materiais e softwares necessários para os treinamentos.

## **Customização**

É sabido que a contratação se dará por meio de “software de prateleira”, ou seja, soluções programadas e produzidas uniformemente e em grande escala, portanto não possuem funcionalidades específicas nem personalizadas, porém, para o Poder Público, a customização de programas de informática é realizada para adaptar softwares às necessidades específicas de um departamento ou usuário, garantindo funcionalidades que atendam requisitos peculiares, sem entretanto, desnaturar ou desvirtuar a utilidade do sistema.

Ainda, a customização permite otimizar processos internos, tornando o software mais eficiente e alinhado aos fluxos de trabalho específicos do órgão público.



# *Câmara Municipal de Carapicuíba*

Estado de São Paulo

Por fim, em alguns casos, a customização é necessária para atender a requisitos legais ou regulamentações específicas de determinados setores, principalmente as questões afetas à legislação local, já que as soluções ofertadas devem atender, primordialmente, a legislação federal e estadual.

## **Prova de Conceito**

A prova de conceito é ferramenta indispensável em processos licitatórios com objetos complexos de inovações e tecnologia da informação, que necessitam de demonstração da viabilidade técnica e funcional da proposta apresentada pelo licitante, antes de sua efetiva contratação. Porém, na contratação em questão ela poderá ser dispensada pois trata-se de solução que já passou por esse processo no passado, e já está em pleno funcionamento e consolidada no ambiente tecnológico.

Como o objeto a ser licitado é vital para o funcionamento da Gestão Pública, principalmente na área administrativa, e não menos importante para a área legislativa, é dever da comissão de avaliação verificar se o objeto a ser entregue atende os requisitos elencados, para que não haja interrupção ou prejuízo das tarefas administrativas diárias relacionadas a solução a ser entregue.

## **4. LEVANTAMENTO DE MERCADO**

O mercado de segurança de endpoints oferece diversas soluções de fabricantes distintos, com diferentes funcionalidades e modelos de licenciamento. Contudo, para a realidade atual da Câmara, a substituição da solução em uso implica projeto de migração, risco de janelas de vulnerabilidade, novos treinamentos e possível perda de histórico de incidentes.

### **Quanto à tecnologia utilizada:**

#### **Cenário 1 – Manter a solução atual**

##### **(1) ESET Protect Endpoint:**

- Renovar/manter as licenças da solução ESET Protect Advanced que já estão em operação e pleno funcionamento na Câmara, preservando a infraestrutura existente de agentes instalados nas estações, console de gerenciamento centralizado e integrações no ambiente tecnológico.

### **Vantagens:**

- Continuidade da solução já implementada, testada e validada pela equipe técnica da Câmara Municipal de Carapicuíba.
- Manutenção da curva de aprendizado da equipe de TI (Sem necessidade de novos treinamentos e novas transferências de conhecimento).



# *Câmara Municipal de Carapicuíba*

Estado de São Paulo

- Consolidação da governança de segurança em uma única plataforma, facilitando auditorias e relatórios.
- Redução de riscos de incompatibilidade, falhas de migração e janelas de vulnerabilidade durante transições dentro do ambiente tecnológico.
- Console de administração em nuvem já integrado à infraestrutura desta Câmara, a partir do qual são geridas as políticas de segurança, inventário de máquinas e notificações de segurança.

## **Desvantagens:**

- Eventual risco de percepção de dependência tecnológica de um único fornecedor, facilmente mitigável com sólida justificativa de adequação de determinada marca às necessidades da Administração conforme análises deste documento e monitoramento periódico do mercado.

## **Cenário 2 - Migração para outra solução de mercado**

### **Vantagens:**

Exploração de outras funcionalidades específicas de mercado, se comprovadamente necessárias à realidade da Câmara Municipal.

### **Desvantagens:**

- Necessidade de projeto de migração, com desinstalação de todos os agentes ESET nos endpoints e instalação de novos agentes, com grande risco de janelas de vulnerabilidade.
- Necessidade de módulos técnicos adicionais para igualar o que a solução atual já entrega de forma consolidada.
- Nova arquitetura técnica da console de gerenciamento e dos agentes instalados nas estações de trabalho.
- Novos treinamentos para a equipe técnica, com grande curva de aprendizado e risco de erros operacionais.
- Possível perda de histórico de incidentes e registros já consolidados na console de administração atual.
- Redesenho das políticas de segurança e regras de detecção de ameaças em um novo console, o que demanda nova validação técnica até que se obtenha nível de segurança equivalente ao ambiente atual.
- Eventual incompatibilidade com a infraestrutura existente ou necessidade de ajustes de rede, políticas e integrações.
- Maior risco de falhas técnicas de configuração e lacunas de proteção na fase de transição para a nova solução.



# *Câmara Municipal de Carapicuíba*

Estado de São Paulo

## **Cenário 3 - Não contratar ou reduzir escopo da proteção**

### **Vantagens:**

- Redução imediata das despesas orçamentárias em TIC.

### **Desvantagens:**

- Aumento substancial do risco de ataques e incidentes de segurança (ransomware, vazamento de dados, indisponibilidade de sistemas).
- A expiração das licenças acarretaria a interrupção dos motores de detecção de ameaças e suas assinaturas, aumentando a exposição a variantes recentes das ameaças cibernéticas.
- Qualquer redução do número de licenças levaria à existência de estações de trabalho sem proteção corporativa compatível com o nível de segurança já implementado, criando pontos de entrada desprotegidos na rede e facilitando sobremaneira os movimentos laterais de ataque.
- Exposição da Câmara a potenciais responsabilizações administrativas, civis e eventualmente penais, caso incidentes resultem de omissão na adoção de controles mínimos razoáveis na segurança da informação.
- A retirada da camada da criptografia de disco integrada à solução atual ou sua aplicação apenas em parte do parque tecnológico aumenta o risco de exposição de dados sensíveis em casos de perda ou furto de equipamentos.
- Desalinhamento das boas práticas de segurança da informação com recomendações de órgãos de controle em matéria de governança de TIC.

## **Quanto à forma de contratação**

Com base no levantamento de mercado e nas experiências de outros órgãos públicos, foram identificados, em linha com a realidade da Câmara Municipal de Carapicuíba, os seguintes cenários possíveis para a forma de contratação da solução de segurança de endpoints:

### **Cenário 1 - Manter a solução atual por contratação direta**

Renovar/manter as licenças da solução ESET Protect Advanced que já estão em operação e pleno funcionamento na Câmara, preservando a infraestrutura existente de agentes instalados nas estações, console de gerenciamento centralizado e integrações no ambiente tecnológico, por meio de contratação direta (preferencialmente por dispensa de licitação), nos termos da Lei nº 14.133/2021, a ser analisada e enquadrada pela Assessoria Jurídica.



# *Câmara Municipal de Carapicuíba*

Estado de São Paulo

## **Vantagens:**

Continuidade da solução já implementada, testada e validada pela equipe técnica da Câmara Municipal de Carapicuíba.

Manutenção da curva de aprendizado da equipe de TI (sem necessidade de novos treinamentos extensivos e novas transferências de conhecimento).

Consolidação da governança de segurança em uma única plataforma, facilitando auditorias, relatórios e a prestação de contas aos órgãos de controle.

Redução de riscos de incompatibilidade, falhas de migração e janelas de vulnerabilidade durante transições dentro do ambiente tecnológico.

Necessidade técnica da Câmara em manter a compatibilidade com a solução de segurança de endpoints já adotada no ambiente tecnológico, em conformidade com o art. 41, inciso I, alíneas “a” e “b”, da Lei nº 14.133/2021.

## **Desvantagem:**

Eventual risco de percepção de dependência tecnológica de um único fornecedor, mitigável com sólida justificativa de adequação de determinada marca às necessidades da Administração e monitoramento periódico do mercado.

## **Cenário 2 - Realizar processo licitatório para migração para outra solução de mercado**

Realizar procedimento licitatório amplo, visando a substituição da solução atual por solução de outro fabricante, com aquisição de novas licenças, implantação de nova console e migração completa do ambiente de segurança de endpoints.

## **Possível Vantagem:**

Exploração de outras funcionalidades específicas de mercado, se comprovadamente necessárias à realidade da Câmara Municipal.

## **Desvantagens:**

Necessidade de projeto de migração, com desinstalação de todos os agentes ESET nos endpoints e instalação de novos agentes, com grande risco de janelas de vulnerabilidade. Novos treinamentos para a equipe técnica, com grande curva de aprendizado e risco de erros operacionais.

Possível perda de histórico de incidentes e registros já consolidados na console de administração atual.



# Câmara Municipal de Carapicuíba

Estado de São Paulo

Eventual incompatibilidade com a infraestrutura existente ou necessidade de ajustes de rede, políticas e integrações.

Maior risco de falhas de configuração e lacunas de proteção na fase de transição para a nova solução.

## **Cenário 3 - Não contratar ou reduzir o escopo de proteção**

Não renovar integralmente as licenças da solução atual ou reduzir significativamente o número de endpoints protegidos.

### **Aparente vantagem:**

Redução imediata das despesas orçamentárias em TIC.

### **Desvantagens:**

Aumento substancial do risco de ataques e incidentes de segurança (ransomware, vazamento de dados, indisponibilidade de sistemas).

Exposição da Câmara a potenciais responsabilizações administrativas, civis e eventualmente penais, caso incidentes resultem de omissão na adoção de controles mínimos razoáveis de segurança da informação.

Desalinhamento com boas práticas de segurança da informação e com recomendações de órgãos de controle em matéria de governança de TIC.

## **4.1. Análise comparativa de soluções – âmbito administrativo**

<b>Indicadores</b>	<b>Cenário 1 Manter a solução atual por contratação direta</b>	<b>Cenário 2 Realizar processo licitatório para migração para outra solução de mercado</b>	<b>Cenário 3 Não contratar ou reduzir o escopo de proteção</b>
<b>VANTAGENS</b>	Continuidade da solução já implementada, testada e validada pela equipe técnica da Câmara Municipal de Carapicuíba.	Exploração de outras funcionalidades específicas de mercado, se comprovadamente necessárias à realidade da Câmara Municipal.	Redução imediata das despesas orçamentárias em TIC.



# Câmara Municipal de Carapicuíba

Estado de São Paulo

	Redução de riscos de incompatibilidade, falhas de migração e janelas de vulnerabilidade durante transições dentro do ambiente tecnológico.	-	-
	Manutenção da curva de aprendizado da equipe de TI (sem necessidade de novos treinamentos extensivos e novas transferências de conhecimento).	-	
	Alinhamento com a necessidade de se manter a compatibilidade com a solução de segurança de endpoints já adotada, com conformidade com o art.41, inciso I, alíneas “b” e “c”m da Lei nº 14.133/2021.	-	-
	Consolidação da governança de segurança em uma única plataforma, facilitando auditorias, relatórios e a prestação de contas aos órgãos de controle.	-	
		-	
<b>DESVANTAGENS</b>	Eventual risco de percepção de dependência tecnológica de um único fornecedor, mitigável com sólida justificativa de adequação de determinada marca às necessidades da	Necessidade de projeto de migração, com desinstalação de todos os agentes ESET nos endpoints e instalação de novos agentes, com grande risco de	Aumento substancial do risco de ataques e incidentes de segurança (ransomware, vazamento de dados, indisponibilidade de sistemas).



# Câmara Municipal de Carapicuíba

Estado de São Paulo

	Administração e monitoramento periódico do mercado.	janelas de vulnerabilidade.	
		Novos treinamentos para a equipe técnica, com grande curva de aprendizado e risco de erros operacionais.	Exposição da Câmara a potenciais responsabilizações administrativas, civis e eventualmente penais, caso incidentes resultem de omissão na adoção de controles mínimos razoáveis de segurança da informação.
		Possível perda de histórico de incidentes e registros já consolidados na console de administração atual.	Desalinhamento com boas práticas de segurança da informação e com recomendações de órgãos de controle em matéria de governança de TIC.
Eventual incompatibilidade com a infraestrutura existente ou necessidade de ajustes de rede, políticas e integrações.			



# Câmara Municipal de Carapicuíba

Estado de São Paulo

## CENÁRIO 1: MANTER A SOLUÇÃO ATUAL POR CONTRATAÇÃO DIRETA

**Vantajosidade Econômica: Há.** A princípio, pois os custos concentram-se na renovação das licenças da solução já implantada, evitando despesas adicionais com projeto de migração, implantação de nova ferramenta, treinamentos extensivos e ajustes de infraestrutura, além de contribuir para reduzir a probabilidade de incidentes de segurança que gerariam custos indiretos elevados.

**Vantajosidade Técnica: Há.** A solução já está implantada, testada e validada; a equipe técnica domina a ferramenta; mantém-se o console único em nuvem, as políticas configuradas, o histórico de incidentes e a governança centralizada da segurança de endpoints, com menor risco operacional e sem janelas de vulnerabilidade decorrentes de migração.

## CENÁRIO 2: REALIZAR PROCESSO LICITATÓRIO PARA MIGRAÇÃO PARA OUTRA SOLUÇÃO DE MERCADO

**Vantajosidade Econômica: Não há.** A princípio, pois além do custo de novas licenças, será necessário investir em projeto de migração, testes, capacitação da equipe técnica e eventuais adequações de infraestrutura, sem que haja, no momento, comprovação de ganho econômico ou funcional que compense o aumento do custo total de propriedade (TCO).

**Vantajosidade Técnica: Não há.** A implementação de nova solução exige desinstalação dos agentes atuais, instalação de novos agentes, reconfiguração de políticas e adaptação de rotinas, com risco de janelas de vulnerabilidade, perda de histórico de incidentes, falhas de configuração e maior probabilidade de erros operacionais durante a transição.

## CENÁRIO 3: NÃO CONTRATAR OU REDUZIR O ESCOPO DE PROTEÇÃO

**Vantajosidade Econômica: Não há.** Embora possa haver redução imediata de despesa com licenças, essa economia é apenas aparente, pois aumenta substancialmente a probabilidade de incidentes de segurança (ransomware, vazamento de dados, indisponibilidade de sistemas), cujos custos de remediação, recuperação e impacto institucional tendem a superar em muito a economia inicial.

**Vantajosidade Técnica: Não há.** A redução ou ausência de licenciamento deixa parte dos endpoints sem proteção adequada, fragiliza controles mínimos de segurança da informação, amplia o risco de incidentes graves e dificulta a governança e a prestação de contas a órgãos de controle, sendo cenário tecnicamente desaconselhável.

### A análise conjunta dos cenários evidencia que:

- O Cenário 1 – manutenção da solução ESET Protect Advanced por contratação direta, com fundamento em manutenção da compatibilidade com os sistemas de segurança já existentes no art. 41, inciso I, alíneas “b” e “c” da Lei nº 14.133/2021 e em necessidade de continuidade do serviço, é o que melhor atende às necessidades atuais da Câmara, do ponto de vista técnico, operacional e de gestão de riscos, ficando o enquadramento jurídico específico (inclusive quanto ao art. 75 da Lei nº 14.133/2021) a cargo da Assessoria Jurídica.



# *Câmara Municipal de Carapicuíba*

Estado de São Paulo

- O Cenário 2 – migração via novo procedimento licitatório apresenta riscos relevantes na fase de transição (janelas de vulnerabilidade, perda de histórico, falhas de configuração e necessidade de ampla capacitação), sem ganho técnico claramente evidenciado para o contexto atual, mostrando-se desvantajoso no momento.
- O Cenário 3 – não contratar ou reduzir o escopo de proteção é tecnicamente desaconselhável, por aumentar significativamente o risco de incidentes de segurança, além de representar potencial omissão na adoção de controles mínimos razoáveis de segurança da informação.

Registram-se, portanto, como alternativas inviáveis:

- a não contratação ou redução relevante da cobertura de proteção de endpoints;
- a migração intempestiva para solução de outro fornecedor, sem motivação técnica robusta e sem planejamento detalhado de transição.

Logo, não atendem as necessidades da Câmara Municipal de Carapicuíba.

Como complemento da comprovação de que a solução mais adequada e eficiente é a manutenção da solução ESET Protect Advanced, segue a análise de alguns produtos existentes no mercado, os quais foram inclusive mencionados pela empresa impugnante nos autos deste processo administrativo, a fim de demonstrar tecnicamente que outras soluções não atendem às necessidades desta Câmara.

As principais plataformas de proteção de endpoints citadas no mercado – como a Bitdefender GravityZone, Sophos Intercept X e Microsoft Defender for Endpoints também são avaliadas de forma positiva por laboratórios independentes de pesquisa na área de segurança da informação. Contudo, para atingir o mesmo escopo de segurança hoje já implantado com o ESET Protect Advanced (proteção de endpoints e servidores, com criptografia completa do disco gerenciada a partir de um console centralizado), essas soluções exigem, em geral a contratação de módulos adicionais e/ou mudanças relevantes no licenciamento, tais como:

- **Bitdefender GravityZone**, necessidade de aquisição de módulo de criptografia de disco completa com licença separada, além do pacote principal de segurança de endpoints, para se obter a criptografia de disco equivalente ao implantado atualmente.
- **Sophos Intercept X**: necessidade de contratação simultânea da solução Intercept X para segurança de endpoints e o módulo Sophos Central Device Encryption, que são produtos separados com licenciamentos adicionais, para gerenciar também a criptografia completa de disco.
- **Microsoft Defender for Endpoints**: Exige atualização para planos mais abrangentes do Microsoft 365 E5 ou aquisições standalone do Defender for



# Câmara Municipal de Carapicuíba

Estado de São Paulo

Endpoint Plan 2, além de licenças adicionais para servidores (Defender for servers), para oferecer o conjunto de funcionalidades semelhante ao implantado atualmente.

Tais alternativas implicariam projetos técnicos de migração essencialmente mais complexos (substituição de agentes, reconfiguração das políticas de criptografia de disco já implantadas e revisão de toda a arquitetura de licenciamento das soluções, sem ganho proporcional em segurança para o cenário específico desta Câmara, considerando que a solução ESET Protect Advanced já se encontra estável em produção, com desempenho e eficácia reconhecidos em testes independentes dos principais laboratórios de segurança da informação disponíveis.

## 4.2. Da fundamentação para indicação da marca ESET

A indicação da marca ESET fundamenta-se no artigo 41, inciso I, alíneas “b” e “c”, da Lei nº 14.133/2021, que autoriza a especificação de marca quando houver necessidade técnica devidamente justificada. Vejamos:

*“Art. 41. No caso de licitação que envolva o fornecimento de bens, a Administração poderá excepcionalmente:*

*I - indicar uma ou mais marcas ou modelos, desde que formalmente justificado, nas seguintes hipóteses:*

*(...)*

*b) em decorrência da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração;*

*c) quando determinada marca ou modelo comercializados por mais de um fornecedor forem os únicos capazes de atender às necessidades do contratante;”*

Sobre isso, a doutrina assim nos ensina:

*“A compatibilidade técnica em razão de padrões, plataformas ou sistemas em funcionamento na Administração Pública representa circunstância autorizadora da indicação de marca/modelo. Tal necessidade de se manter uma compatibilidade técnica é comumente constatada no campo da informática. De qualquer forma, torna-se imprescindível um parecer técnico que fundamente esta circunstância, podendo, em certos casos, resultar até mesmo em uma inexigibilidade de licitação em razão do fornecedor ou produtor exclusivo.*

*A lei ainda prescreve que, quando apenas uma marca ou modelo comercializados por diversos particulares forem os únicos capazes de atender à certa demanda, a indicação no edital da licitação é possível, pois não haverá a frustração da competição, tendo em vista a existência de uma pluralidade de possíveis*



# Câmara Municipal de Carapicuíba

Estado de São Paulo

*fornecedores.”* (Manual de Licitações e Contratos Administrativos, Editora Forense, 3ª Edição, Coordenação Maria Sylvia Zanella Di Pietro)

E mais:

*“Outra hipótese de indicação de marca envolve a necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração.*

*Notadamente na área de tecnologia da informação, as aquisições devem ser feitas de maneira refletida. Diante da adoção de uma determinada plataforma, não faz sentido adquirir equipamentos incompatíveis com ela, com utilização prática imprestável.*

*Uma terceira hipótese de indicação ocorre quando determinada marca ou modelo comercializados por mais de um fornecedor forem os únicos capazes de atender às necessidades do contratante.*

*A motivação técnica, para justificar a incidência de tal exceção, deve ser claramente descrita, de forma a demonstrar sua indispensabilidade para a execução do objeto pretendido, além de ser confirmada pela autoridade competente. A indicação de marca como única apta a atender a pretensão contratual da Administração é possível, contudo, "deve estar amparada em razões de ordem técnica, de forma motivada e documentada, que demonstrem ser aquela marca específica a única capaz de satisfazer o interesse público".* (Leis de LICITAÇÕES PÚBLICAS comentadas, Editora Juspodivm, 14ª Edição, Autor Ronny Charles Lopes de Torres)

No caso em análise, a solução ESET Protect Advanced já é utilizada pela Câmara Municipal de Carapicuíba há aproximadamente três anos, estando plenamente integrada à infraestrutura de tecnologia da informação da Casa. Trata-se da plataforma atualmente responsável pela segurança dos computadores e demais equipamentos (endpoints), por meio de console centralizado de gerenciamento em nuvem, com políticas de segurança já configuradas, agentes instalados em todos os equipamentos e histórico de registros e incidentes acumulados ao longo do período de uso.

A adoção de solução de outro fabricante implicaria a perda dessa compatibilidade, exigindo a desinstalação dos agentes atualmente em funcionamento, a implantação de nova plataforma, a reconfiguração integral das políticas de segurança, além da interrupção do histórico de dados já existente. Esse processo traria riscos operacionais relevantes, inclusive a criação de períodos de vulnerabilidade na segurança da informação, o que não se mostra recomendável para a Administração.



# *Câmara Municipal de Carapicuíba*

Estado de São Paulo

Assim, a manutenção da solução ESET mostra-se necessária para garantir a continuidade dos serviços de segurança da informação, preservar a estrutura já implantada, evitar riscos desnecessários e aproveitar os investimentos já realizados em licenças, configurações e capacitação da equipe técnica. Trata-se, portanto, de hipótese prevista no artigo 41, inciso I, alínea “b”, da Lei nº 14.133/2021, que autoriza a especificação de marca para fins de compatibilidade com padrões já adotados.

Além disso, conforme previsto no artigo 41, inciso I, alínea “c”, a marca ESET é a única que atende integralmente às necessidades atuais da Câmara, considerando o contexto operacional existente. Embora existam outras soluções no mercado, a substituição da plataforma implicaria custos adicionais, necessidade de novos treinamentos, maior risco de falhas na transição e prejuízos à continuidade do serviço.

Precisaríamos desinstalar e reinstalar proteção em 80 computadores, com risco de ficar desprotegidos durante o processo; a equipe precisaria de novos treinamentos extensos, com risco de erros; poderíamos perder o histórico de incidentes já registrado; poderia haver incompatibilidade com outros sistemas da Câmara e maior risco de falhas na configuração inicial.

Ressalta-se, ainda, que a solução ESET é comercializada por diversos fornecedores autorizados, o que possibilita a realização de procedimento competitivo, sem prejuízo aos princípios da economicidade e da competitividade.

Dessa forma, conclui-se que a especificação da marca ESET encontra amparo legal e técnico, sendo medida adequada para garantir a continuidade dos serviços, a segurança da informação e a eficiência administrativa, em conformidade com o artigo 41, inciso I, alíneas “b” e “c”, da Lei nº 14.133/2021, e alinhada aos princípios da eficiência, economicidade e continuidade do serviço público previstos no artigo 37 da Constituição Federal e artigo 5º da Lei nº 14.133/2021.

Ressalta-se que, inicialmente, o presente processo foi instaurado com fundamento equivocado na alínea “a” do inciso I do artigo 41 da Lei nº 14.133/2021, que trata da especificação de marca em razão de padronização. Nessa hipótese, a legislação exige a prévia instauração de processo formal de padronização, nos termos do artigo 43 da referida lei.

Contudo, após análise e parecer jurídico da Procuradora da Câmara, foi apontada a necessidade de reavaliação do enquadramento legal do objeto, uma vez que a contratação pretendida não se caracteriza como padronização de bens ou serviços para uso futuro e amplo pela Administração, mas sim como manutenção de solução já implantada e em pleno funcionamento.

Diante dessa orientação da Procuradoria, o objeto foi revisto pela área técnica, verificando-se que a justificativa para a indicação da marca não se enquadra na alínea “a” do inciso I do artigo 41, mas, de forma mais adequada, nas alíneas “b” e “c” do mesmo dispositivo legal, que tratam, respectivamente, da necessidade de compatibilidade com



# *Câmara Municipal de Carapicuíba*

Estado de São Paulo

plataformas e padrões já adotados pela Administração e da existência de marca específica capaz de atender integralmente às necessidades do contratante.

Assim, concluiu-se que não há necessidade de instauração de processo de padronização no presente caso, uma vez que a escolha da marca não decorre de decisão administrativa de padronizar produtos ou sistemas, mas de necessidade técnica objetiva, relacionada à continuidade do serviço, à preservação da infraestrutura existente e à mitigação de riscos operacionais.

Dessa forma, a indicação da marca encontra-se tecnicamente e devidamente justificada no âmbito deste Estudo Técnico Preliminar, em conformidade com o artigo 41, inciso I, alíneas “b” e “c”, da Lei nº 14.133/2021, não se aplicando, portanto, o disposto no artigo 43 da mesma lei.

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

A solução a ser contratada consiste na manutenção/renovação da solução de segurança de endpoints ESET Protect Advanced, contemplando:

- Licenças para proteção de aproximadamente 75 endpoints (estações de trabalho, notebooks e servidores);
- Console de gerenciamento em nuvem para administração centralizada;
- Funcionalidades de proteção avançada contra ameaças (ransomware, zero-day, malware avançado);
- Recursos de inventário e relatórios de auditoria e conformidade;
- Suporte técnico para o ambiente já implantado.

A solução integra-se à infraestrutura de TI existente da Câmara e está em operação há cerca de 3 anos, com curva de aprendizado consolidada pela equipe técnica.

## **6. ESTIMATIVA DAS QUANTIDADES**

Com base no estudo técnico, estima-se a necessidade de aproximadamente 75 licenças da solução ESET Protect Advanced, distribuídas entre estações de trabalho, notebooks, servidores e demais ativos críticos mapeados pela área de TI.

O quantitativo final deverá ser ajustado conforme levantamento atualizado de ativos de TI da Câmara no momento da formalização da contratação, mantendo a diretriz de cobertura integral dos ativos relevantes.



# Câmara Municipal de Carapicuíba

Estado de São Paulo

## 7. ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Estamos utilizando como referência as cotações obtidas junto a três empresas especializadas nos produtos do fabricante ESET. Essas informações compõem a base para a formação de preço, garantindo aderência às exigências estabelecidas pela Lei nº 14.133/2021. Conforme previsto na legislação, a apresentação de pesquisas de mercado realizadas com fornecedores qualificados é requisito essencial para a elaboração do Estudo Técnico Preliminar. Dessa forma, asseguramos transparência, confiabilidade e alinhamento técnico no processo de contratação.

EMPRESA	DESCRIÇÃO	VALOR UNIT.	VALOR TOTAL
UNITEC SOLUCOES EM TI LTDA	ESET PROTECT ADVANCED + SUPORTE E MON.	R\$ 333,33	R\$ 25.000,00
SOCIETY INFORMATICA COM. LTDA	ESET PROTECT ADVANCED + SUPORTE E MON.	R\$ 344,30	R\$ 25.822,50
GO UP INFORMATICA LTDA	ESET PROTECT ADVANCED + SUPORTE E MON.	R\$ 515,33	R\$ 38.650,00
<b>MÉDIA</b>			<b>R\$ 29.824,17</b>

## 8. JUSTIFICATIVA PARA PARCELAMENTO

Tratando-se de solução integrada de segurança de endpoints, baseada em console único de gerenciamento e consolidação da proteção em todos os endpoints e necessidade de governança centralizada, a contratação em lote único mostra-se a forma mais adequada para evitar fragmentação da proteção entre múltiplas soluções ou fornecedores, assegurar uniformidade de políticas de segurança e simplificar a gestão contratual e a fiscalização da execução.

A necessidade de contratação da solução ESET Protect Advanced como solução integrada de segurança de endpoints fundamenta tecnicamente a opção pelo não parcelamento do objeto.

## 9. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

A solução de segurança de endpoints integra a arquitetura de TI da Câmara e guarda relação com outros sistemas e serviços de TIC (como redes, sistemas de gestão, infraestrutura de servidores, entre outros).

Eventuais contratos correlatos (por exemplo, de suporte de infraestrutura, redes ou serviços de TI) devem ser verificados pela área responsável e, se pertinente, registrados



# *Câmara Municipal de Carapicuíba*

Estado de São Paulo

no processo como contratações interdependentes, para garantir alinhamento entre prazos de vigência, assegurar coerência na estratégia de segurança da informação e evitar lacunas de proteção.

## **10. ALINHAMENTO COM PLANO DE CONTRATAÇÕES ANUAL (PCA)**

Nos termos das boas práticas de planejamento previstas na Lei nº 14.133/2021 e nas normas internas da Câmara, a manutenção da solução de segurança de endpoints deverá estar alinhada ao Plano de Contratações Anual (PCA), seja por já constar como necessidade de TIC para o exercício correspondente, seja mediante inclusão/ajuste em ciclo de revisão do PCA.

Esse alinhamento reforça a previsibilidade orçamentária, a governança de TIC e a transparência na gestão de contratações.

## **11. DEMONSTRAÇÃO DOS RESULTADOS PRETENDIDOS**

A manutenção da solução ESET PROTECT Advanced busca alcançar, entre outros, os seguintes resultados:

- Continuidade da proteção de endpoints e servidores, com redução do risco de incidentes de segurança.
- Governança consolidada da segurança de endpoints em console único de gerenciamento em nuvem.
- Manutenção da curva de aprendizado da equipe técnica, evitando custos adicionais e riscos decorrentes de mudanças abruptas de solução.
- Redução de janelas de vulnerabilidade, ao evitar projetos de migração complexos e desnecessários no curto prazo.
- Facilitação da prestação de contas aos órgãos de controle, por meio de relatórios consolidados e histórico de incidentes.
- Alinhamento às boas práticas de gestão de riscos em TIC.

## **12. PROVIDÊNCIAS PRÉVIAS AO CONTRATO OU EQUIVALENTE**

Para mitigar riscos identificados no estudo, especialmente o risco de interrupção de cobertura por atraso na contratação, recomenda-se:

- Planejar a contratação com antecedência, observando a data de término das licenças atuais;



# *Câmara Municipal de Carapicuíba*

Estado de São Paulo

- Acompanhar cronograma interno de tramitação do processo;
- Atualizar o levantamento de ativos protegidos para dimensionamento preciso de licenças;
- Submeter o processo à Assessoria Jurídica para análise de enquadramento da hipótese de contratação.

## **13. IMPACTOS AMBIENTAIS**

Considerando que se trata de manutenção de solução de software já implantada, sem aquisição de novos equipamentos físicos, não se identificam impactos ambientais relevantes adicionais decorrentes desta contratação.

A solução contribui indiretamente para a sustentabilidade ao reduzir riscos de perda de dados e necessidade de retrabalho, apoiando a continuidade do serviço público com uso eficiente da infraestrutura de TI existente.

## **14. VIABILIDADE DA CONTRATAÇÃO**

O estudo técnico conclui que a contratação para manutenção da solução ESET Protect Advanced é tecnicamente viável, pois a solução já está implantada, testada e em operação, atendendo às necessidades de proteção e governança de segurança da informação.

A contratação mostra-se operacionalmente adequada, uma vez que a equipe técnica domina os procedimentos de instalação, configuração, monitoramento e resposta a incidentes na plataforma, e o fluxo de trabalho está estruturado com base nessa solução.

A eventual contratação direta (dispensa de licitação) possui natureza excepcional e dependerá de enquadramento jurídico específico com fundamento no art. 75 da Lei nº 14.133/2021, cabendo à Assessoria Jurídica a análise da hipótese aplicável. O presente ETP não substitui tal enquadramento, limitando-se à recomendação técnica.

## **15. ANEXOS**

15.1. Anexo I – Análise de Risco.

## **16. RESPONSÁVEIS**

Carapicuíba, 9 de janeiro de 2026.

**JEREMIAS ANTUNES DE OLIVEIRA**  
Setor de Compras



# Câmara Municipal de Carapicuíba

Estado de São Paulo

## ANEXO I

### ANÁLISE DE RISCO

Contratação de empresa especializada em Segurança da Informação para a renovação da solução de endpoint antivírus ESET PROTECT Advanced, com período de licenciamento de 36 (trinta e seis) meses, incluindo suporte técnico especializado 8x5 (oito horas por dia, cinco dias por semana), console de gerenciamento em nuvem (cloud) e, monitoramento 24x7 (tempo integral) conforme especificações constantes no Termo de Referência.

Fase	Interna		
Situação	Interrupção de cobertura de segurança por atraso na contratação		
Probabilidade	<input type="checkbox"/> Baixa	<input type="checkbox"/> Média	<input checked="" type="checkbox"/> Alta
Impacto	<input type="checkbox"/> Baixo	<input type="checkbox"/> Médio	<input checked="" type="checkbox"/> Alto
Plano de mitigação	Planejar a contratação com antecedência; acompanhar cronograma; prever prazo hábil para tramitação do processo e eventual migração de licenças.		
Responsáveis	Setor de TI, Diretoria Geral, Setor de Compras e Licitações, Contabilidade, Jurídico e Presidência.		

Fase	Interna		
Situação	Não atendimento de requisitos legais/procedimentais na contratação direta		
Probabilidade	<input type="checkbox"/> Baixa	<input checked="" type="checkbox"/> Média	<input type="checkbox"/> Alta
Impacto	<input type="checkbox"/> Baixo	<input type="checkbox"/> Médio	<input checked="" type="checkbox"/> Alto
Plano de mitigação	Submeter o processo à Assessoria Jurídica; observar rigorosamente as exigências do art. 75 da Lei nº 14.133/2021; elaborar pesquisa de preços adequada; instruir o processo com ETP, parecer jurídico e demais documentos exigidos.		
Responsáveis	Setor de TI, Diretoria Geral, Setor de Compras e Licitações, Jurídico e Presidência.		



# Câmara Municipal de Carapicuíba

Estado de São Paulo

Fase	Execução		
Situação	Incidentes de segurança graves (ransomware, vazamento de dados)		
Probabilidade	<input type="checkbox"/> Baixa	<input checked="" type="checkbox"/> Média	<input type="checkbox"/> Alta
Impacto	<input type="checkbox"/> Baixo	<input type="checkbox"/> Médio	<input checked="" type="checkbox"/> Alto
Plano de mitigação	Manter solução corporativa robusta já implantada no ambiente tecnológico; revisar periodicamente políticas; realizar campanhas internas de conscientização e testes de resposta a incidentes.		
Responsáveis	Setor de TI.		

Fase	Execução		
Situação	Falhas operacionais decorrentes de mudança de solução		
Probabilidade	<input type="checkbox"/> Baixa	<input type="checkbox"/> Média	<input checked="" type="checkbox"/> Alta
Impacto	<input type="checkbox"/> Baixo	<input type="checkbox"/> Médio	<input checked="" type="checkbox"/> Alto
Plano de mitigação	Em caso de futura revisão da solução contratada, planejar projeto de migração gradual com testes, homologação e treinamentos; atualmente, a manutenção da solução reduz esse risco.		
Responsáveis	Setor de TI, Diretoria Geral e Presidência.		

Fase	Execução		
Situação	Dependência excessiva de fornecedor específico		
Probabilidade	<input type="checkbox"/> Baixa	<input checked="" type="checkbox"/> Média	<input type="checkbox"/> Alta
Impacto	<input type="checkbox"/> Baixo	<input checked="" type="checkbox"/> Médio	<input type="checkbox"/> Alto
Plano de mitigação	Monitorar periodicamente o mercado; registrar em plano de TIC a possibilidade de reavaliar a implementação da solução em ciclos definidos ou quando do vencimento do licenciamento da solução atual (ex.: a cada 3 anos); manter documentação técnica organizada para viabilizar eventual futura migração.		
Responsáveis	Setor de TI.		