AVISO DE DISPENSA DE LICITAÇÃO 34/2025

COM BASE NO §3º DO ART. 75 DA LEI N. 14.133/2021 E NO INCISO VI DO ART. 35 DO ATO DA MESA Nº 7, DE 11 DE DEZEMBRO DE 2023

A Câmara Municipal de Carapicuíba, com sede na Travessa Virgínio Pasini, n° 63 - Jardim Sao Pedro, Carapicuíba - SP, CEP 06320-000, neste ato representado pelo seu agente de contratação, designado pela Portaria Nº 068/2025, 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 neste Termo de Referência em anexo.

Limite para apresentação da Proposta de Preços: dia 28 de janeiro de 2026, até às 18 horas.

A Solicitação de Proposta da contratação encontra-se disponível nos anexos desta Publicação.

A proposta deverá ser entregue no Setor de Compras e Licitações cito Travessa Virgínio Pasini, n° 63 - Jardim Sao Pedro, Carapicuíba - SP, 06320-000 ou pelo email: compras@camaracarapicuiba.sp.gov.br

SOLICITAÇÃO DE PROPOSTA COMERCIAL

A Câmara Municipal de Carapicuíba solicita cotações de preços para 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 neste Termo de Referência em anexo.

A proposta deverá conter:

- Descrição do objeto, valor unitário e total;
- Número do Cadastro de Pessoa Física - CPF ou do Cadastro Nacional de Pessoa Jurídica - CNPJ do proponente;
- Endereço físico, eletrônico e telefone de contato;
- Data de emissão;
- Nome completo e identificação do responsável;
- Validade da Proposta: Mínima de 90 dias;
- Prazo de entrega: De até 10 (dez) dias;
- Condições de pagamento: Em até 5 (cinco) dias, após entrega e aprovação.

Fico à disposição para eventuais esclarecimentos.

Atenciosamente,

Gabriela da Silva Nascimento – Setor de Compras
Câmara Municipal de Carapicuíba
Tv. Virgínio Pasini, 63 – Jardim São Pedro – Carapicuíba/SP – CEP 06320-000
Tel.: 3536-8854
CNPJ: 49.759.954/0001-71

TERMO DE REFERÊNCIA

1. UNIDADE SOLICITANTE

1.1. Setor de Informática

2. OBJETO

2.1. 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 neste Termo de Referência.

3. JUSTIFICATIVA

3.1. A renovação da solução de antivírus se faz necessária em razão do término do contrato atual o qual, conforme a legislação aplicável (Lei nº 14.133/2021), se enquadra no inciso I do artigo 41, alíneas “b” e “c”, que tratam respectivamente, da necessidade de compatibilidade com plataformas e padrões já adotados pela Administração e da existência de marca específica capaz de atender integralmente às necessidades do contratante.

3.2. Conforme Estudo Técnico Preliminar concluiu-se que não há necessidade de instauração de processo de padronização na presente contratação, 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.

3.3. Dessa forma, a indicação da marca encontra-se tecnicamente e devidamente justificada no âmbito deste processo, 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.

3.4. Considerando a crescente demanda por segurança da informação e a necessidade de proteção contínua contra ameaças cibernéticas, a contratação abrangerá o fornecimento de solução antivírus com console em nuvem, suporte técnico especializado em regime 8x5 e monitoramento do ambiente em regime 24x7, garantindo maior visibilidade, controle centralizado e respostas rápidas a incidentes. A medida visa assegurar a integridade, confidencialidade e disponibilidade dos dados institucionais, em conformidade com as boas práticas de governança e com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

3.5. A contratação da licença de antivírus por 36 meses, ao invés de um prazo mais curto, é justificada por benefícios econômicos e operacionais, tais como:

3.5.1 **Economia de escala:** A obtenção de um contrato de longo prazo costuma possibilitar a obtenção de um preço mais baixo em relação à renovação anual.

3.5.2. **Previsibilidade orçamentária:** Um contrato de 36 meses possibilita a fixação do valor da licença por um período extenso, resguardando a Cãmara contra futuros aumentos de preços e simplificando o planejamento financeiro.

3.5.3. **Diminuição de despesas administrativas:** a redução do número de processos de compra resulta em menor tempo e recursos gastos em licitações e negociações anuais, permitindo que a equipe administrativa se dedique a outras atividades.

3.5.4. **Gestão de segurança simplificada**: Um contrato de longo prazo possibilita uma administração da segurança cibernética mais estável e eficiente. A equipe de TI não precisa se preocupar com a expiração da licença, podendo concentrar-se na implementação de políticas de segurança e no monitoramento constante.

3.5.5. **Melhor aproveitamento da solução**: A utilização de uma solução por um período mais longo permite que a equipe se familiarize com todas as suas funcionalidades, o que melhora a eficácia da ferramenta e a capacidade de resposta a incidentes de segurança.

3.6. O investimento é fundamental para a manutenção da segurança digital, continuidade operacional e conformidade legal da instituição, refletindo diretamente na qualidade dos serviços prestados e na confiança da população quanto à proteção das informações públicas.

4. ESPECIFICAÇÃO E QUANTITATIVO

ITEM	DESCRIÇÃO	PERIODO	QTD	TIPO
1.	**Licenciamento e Serviços**			
1.1.	**Renovação** da solução de antivírus ESET PROTECT Advanced.	36 meses	75	Licenciamento
1.2.	**Serviço** de suporte técnico, atendimento 8x5 (oito horas por dia, cinco dias por semana), console de gerenciamento em nuvem e monitoramento 24x7 (tempo integral)	36 meses	01	Serviço

4.1. ESPECIFICAÇÕES TÉCNICAS

4.1.1. CONSOLE DE GERENCIAMENTO EM NUVEM

4.1.1.1. A solução deve dispor de console de gerenciamento com administração centralizada, auxiliando na questão de instalação, administração, atualização, configuração e monitoramento com cada um de seus módulos advindos de um único fornecedor;
4.1.1.2. A console de gerenciamento deve ser acessada através de tecnologia via conexão segura (HTTPS) compatível com os navegadores Google Chrome, Microsoft Edge, Mozilla Firefox, Opera e Safari;

4.1.1.3. A console de gerenciamento deve suportar sessões simultâneas entre os usuários que a ela possuem acesso;

4.1.1.4. Será de responsabilidade da CONTRATADA implementar e configurar toda a estrutura contratada pela CONTRATANTE na console de gerenciamento em nuvem;

4.1.1.5. O Data Center deverá atender no mínimo às certificações Tier III ou ISO27001 ou SOC 2 Type 2;

4.1.1.6. O licenciamento e operação do ambiente em nuvem é de total responsabilidade da CONTRATADA;

4.1.1.7. A CONTRATADA deverá garantir a segurança da informação dos dados e estrutura em nuvem que irá hospedar os dados da CONTRATANTE;

4.1.1.8. O data center deverá estar hospedado em São Paulo para evitar problemas de latência de dados;

4.1.1.9. A console de gerenciamento em cloud deverá ter a tecnologia de duplo fator de autenticação para acessar o ambiente computacional em cloud e a função deverá ser do próprio não sendo aceito autenticador de terceiros.

4.1.1.10. As instalações físicas do data center deverão ter os seguintes itens:
- Sistema de piso elevado, com vias independentes de cabos de energia, lógicos e óticos;
- Deverá possuir vias de energia elétrica e lógica em alta disponibilidade;
- Sistema de proteção contra descargas eletromagnéticas, descargas atmosféricas e aterramento.

4.1.1.11. A estrutura de energia elétrica do data center deverá atender aos seguintes requisitos:

4.1.1.11.1. Alimentação elétrica redundante;
- Total independência no fornecimento de energia na eventualidade de falha na subestação que atende ao data center;
- Solução de grupo gerador redundante e independente (n+1), com acionamento automático na eventualidade de interrupção no fornecimento de energia e com capacidade mínima de funcionamento por 72 horas com combustível local;
- Mínimo de 2KVAs nominais;
- Alimentação elétrica redundante e independente para os equipamentos da solução.

4.1.1.12. O data center que aloca o ambiente computacional da CONTRATANTE deverá atender os seguintes requisitos de climatização:
- Sistema de climatização com controles de temperatura, umidade relativa do ar e filtros de poeira;
- Sistema de climatização redundante (n+1), refrigerado por formas diferentes;

- Temperatura constante de 20ºC +/- 2ºC e umidade relativa do ar constante de 50% +/-10%.

4.1.1.13. O data center que aloca o ambiente computacional da CONTRATANTE deverá atender os seguintes requisitos de proteção contra incêndio:

- Dispositivos tradicionais de prevenção e combate a incêndio (brigada de incêndio, extintores manuais e detectores de fumaça);
- Sistema automático de extinção de incêndios, baseado em agentes gasosos não poluentes, com ação baseada na quebra das moléculas de Oxigênio, do tipo FM200 e/ou FE227, ou equivalente, não nocivos aos equipamentos e seres humanos e que atenda a padrões internacionais;
- Sistema de detecção de incêndio por sensores termovelocimétricos para a sala dos servidores do data center, tipo VESDA, ou equivalente; possuir dispositivos de detecção precoce de incêndio pela análise do superaquecimento de cabos ou hardwares que sejam de maior sensibilidade que os tradicionais detectores de fumaça;
- Possuir sistema de detecção de incêndio por sensores termovelocimétricos para os ambientes de servidores e de armazenamento de dados;
- Possuir os componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes.

4.1.1.14. O data center que aloca o ambiente computacional da CONTRATANTE deverá possuir os seguintes requisitos de segurança física:

- Disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos;
- Mecanismos efetivos de controle de entrada e saída de pessoas que acessem e façam uso do IDC, bem como de registros passíveis de posterior pesquisa;
- Capacidade de cadastro remoto de usuários para acesso ao data center;
- Deverá possuir a capacidade de cadastro de novo usuário local com permissão do administrador;
- Acesso ao local através de leitura biométrica;
- Possuir alerta por SMS e e-mail em tempo real de acesso ao ambiente;
- Arquivar as imagens gravadas pelas câmeras de vídeo de segurança por pelo menos 30 (trinta) dias;
- O Datacenter deverá possuir vigilância patrimonial 24 horas por dia, 7 dias por semana, 365 dias por ano, permitindo apenas a entrada de pessoas autorizadas e devidamente identificadas;
- Possuir metodologia para classificação e controle de ativos e de acessos ao ambiente do Datacenter;
- Acondicionar equipamentos e mídias geradas no ambiente do Datacenter, livres de riscos físicos;
- Possuir rígido controle de acessos aos equipamentos do Datacenter, mesmo por pessoas credenciadas pela CONTRATANTE;
- Disponibilizar mecanismos efetivos de controle de entrada e saída de pessoas, que acessam ou façam uso do Datacenter, com leitores biométricos ou cartões magnéticos individuais;
- Possuir travas eletrônicas que, de acordo com a política de segurança estabelecida para o Datacenter, a dívida em regiões com níveis de restrição diferenciados;
- Possuir sistema de detectores de movimento no ambiente.

4.1.1.15. O mecanismo utilizado pela console de gerenciamento é o push, para comunicação em tempo real entre o servidor e os clientes para aplicação das configurações e entrega de licenças.

4.1.1.16. A console de gerenciamento deve permitir o agrupamento dos computadores em sites, domínios e grupos, e sua administração ser individualizada por domínio.

4.1.1.17. O servidor de gerenciamento da solução deve possuir compatibilidade para instalação nos seguintes sistemas operacionais e suas versões (Incluindo distribuições, releases e seus hypervisors):

- Microsoft Windows 10;
- Microsoft Windows 11;
- Microsoft Windows Server 2012R2;
- Microsoft Windows Server 2016;
- Microsoft Windows Server 2019;
- Microsoft Windows Server 2022;
- Microsoft Windows Server 2025;
- Debian 10 x64;
- Debian 11 x64;
- Ubuntu 20.04LTS x64;
- Rocky Linux 9;
- RHEL Server 8 x64;
- VMware vSphere/ESXi 6.5 e posteriores;
- VMware Workstation 9 e posteriores;
- VMware Player 7 e posteriores;
- Microsoft Hyper-V Server 2012, 2012R2, 2016, 2019, 2022;
- Citrix 7.0 e posteriores;
- Oracle VirtualBox 6.0 e posteriores;

4.1.1.18. O servidor de gerenciamento da solução deve possuir compatibilidade para instalação de sistemas de arquitetura 64 bits nos ambientes virtual e físico, a ser disponibilizado pela CONTRATANTE.

4.1.1.19. A console de gerenciamento deve oferecer gerenciamento em nuvem, a ser disponibilizado pela CONTRATADA.

4.1.1.20. O servidor de gerenciamento da solução deve possuir integração com Active Directory e LDAP para importação da estrutura organizacional que será replicada na console de gerenciamento.

4.1.1.21. A console de gerenciamento deve permitir a adoção e aplicação de regras diferenciadas que serão baseadas na localidade lógica da rede.

4.1.1.22. A console de gerenciamento deve permitir a criação de grupos com regras distintas para cada dispositivo.

4.1.1.23. A solução deve permitir a instalação dos clientes de comunicação em estações de trabalho e servidores sendo estes físicos ou virtualizados, através da console de gerenciamento remota sem intervenção e/ou interação do usuário (Modo silencioso).

4.1.1.24. A solução deve permitir a remoção automatizada das soluções de outros fabricantes que estejam instaladas nas estações de trabalho e/ou servidores da **CONTRATANTE.**

4.1.1.25. A solução deve possuir a funcionalidade de varredura da rede para descoberta das estações e servidores que não possuem o cliente instalado através da console de gerenciamento.

4.1.1.26. A solução deve fornecer uma ferramenta para a pesquisa de estações e servidores que não possuem o cliente instalado, fornecendo a opção de instalação remota através de console de gerenciamento.

4.1.1.27. A console de gerenciamento deve possuir funcionalidade que impeça o usuário de alterar as configurações do cliente instalado na máquina que está sendo gerenciada, de modo que não possa ALTERAR, IMPORTAR e EXPORTAR configurações, ABRIR a console do cliente instalado e DESINSTALAR ou PARAR a execução do serviço do cliente instalado.

4.1.1.28. A console de gerenciamento deve possuir a capacidade de criação de contas de usuário de administração com diferentes perfis de acesso (De forma a possuir ao menos os perfis de operador da console e administrador).

4.1.1.29. A solução deve possuir sistema baseado em método RBAC (Role Based Access Control) para definição de acessos customizados dos usuários que farão uso da console de gerenciamento, oferecendo níveis de granularidade para configuração destes acessos de forma a criar uma segregação e limitá-los, se aplicando, mas não somente a POLÍTICAS, TAREFAS e demais objetos do console de gerenciamento.

4.1.1.30. A console de gerenciamento deve possuir log centralizado com as seguintes informações:

- Nome da ameaça encontrada;
- Nome do arquivo infectado;
- Caminho da detecção;
- HASH do arquivo;
- Data e hora da infecção;
- Ação de mitigação tomada;
- Endereço IP da máquina;
- Usuário autenticado na máquina;
- Origem da ameaça (Hostname ou endereço IP da máquina) caso a ameaça tenha se propagado.

4.1.1.31. A console de gerenciamento deve fornecer em tempo real o status atualizado das estações de trabalho e servidores gerenciados, contendo ao menos as seguintes informações:

- Nome da máquina;
- Endereço IP da máquina;
- Malwares não removidos;
- Ameaças encontradas;
- Status da conexão;
- Data da vacina contra vulnerabilidades;
- Versão da solução antivírus instalada.

4.1.1.32. A console de gerenciamento deve prover alertas de segurança através do envio de emails, com informações de infecções de máquinas e ataques cibernéticos, de forma a conter ao menos as seguintes informações:

- Detecções de Malware;
- Detecções de Firewall;
- Detecções via EDR;

4.1.1.33. O console de gerenciamento deve utilizar o protocolo HTTPS para comunicação entre o cliente instalado e a própria console.

4.1.1.34. A solução deve fornecer alternativa de rollback de versões anteriores (Solução de antivírus ou suas vacinas) conforme procedimento específico na console de gerenciamento.
4.1.1.35. A interface da console de gerenciamento deve fornecer a opção de linguagem totalmente traduzida para português Brasileiro.

4.1.1.36. A console deve ser capaz de funcionar através de um appliance virtual, com imagem a ser fornecida pelo fabricante.

4.1.1.37. O acesso a console de administração deve permitir o uso de MFA (Múltiplo fator de autenticação) a ser configurado na própria console sem que haja a obrigatoriedade da instalação de add-ons.

4.1.1.38. A solução deve possuir integração com Microsoft Entra ID para login único na console de gerenciamento com uso de Single Sign On (SSO).

4.1.1.39. A solução deve ser capaz de prover pacotes de instalação para os sistemas operacionais existentes na estrutura corporativa do CONTRATANTE, de forma a permitir a gravação em mídias removíveis e instalação do software em ambientes onde não seja possível a instalação através da rede corporativa.

4.1.1.40. A solução deve permitir que a instalação do software cliente do antivírus seja feita de forma forçada nas estações, de forma a efetuar a reinstalação automaticamente caso haja a desinstalação ou corrupção do cliente atualmente instalado.

4.1.1.41. A solução deve realizar o gerenciamento de todos os clientes instalados nas máquinas da empresa (Estações de trabalho, servidores, tablets e smartphones) a partir da console de gerenciamento, oferecendo a possibilidade da centralização das configurações e das funcionalidades.

4.1.1.42. A solução deve gerenciar e sobrescrever de forma remota as configurações do firewall local de cada máquina que possua o cliente instalado.

4.1.1.43. A solução deve oferecer recurso de isolamento das máquinas da rede, de forma a manter apenas a comunicação essencial e segura com o servidor de gerenciamento.

4.1.1.44. A solução deve permitir a criação de regras de exceção de isolamento de rede, de forma a permitir somente a comunicação com IPs específicos da rede neste período.

4.1.1.45. A solução deve possuir a funcionalidade de recurso de criação de grupos e subgrupos de máquinas baseado na hierarquia do Active Directory e LDAP utilizando identificador único para os clientes, como o endereço IP.

4.1.1.46. A solução deve permitir que as configurações determinadas no servidor de gerenciamento sejam aplicadas de forma forçada para as estações, protegendo assim a alteração por parte dos usuários, com a utilização de senha determinada previamente.
4.1.1.47. A solução deve permitir a atualização e sincronização das configurações para os clientes sem a necessidade de reinicialização ou logoff.

4.1.1.48. A solução deve permitir a criação de tarefas para rastreamento de malwares em períodos pré-determinados e durante a inicialização do sistema operacional das estações.

4.1.1.49. A solução deve permitir a criação de tarefas para atualização das vacinas de proteção e novas versões de software em períodos pré-determinados.

4.1.1.50. A solução deve possuir ferramentas que permitam o gerenciamento e distribuição centralizados de atualização e distribuição dos softwares e seus módulos, não sendo permitido de nenhuma forma o uso de ferramentas de terceiros para essa finalidade.

4.1.1.51. A solução deve permitir a criação de tarefas para somente uma máquina, um grupo determinado de máquinas e/ou para todas as máquinas.

4.1.1.52. A solução deve possuir no mínimo 50 modelos de relatórios com configuração prévia utilizando filtros e conjunto de filtros na console de gerenciamento.

4.1.1.53. A console de gerenciamento na nuvem deve permitir a criação de relatórios customizados. Não serão aceitos apenas relatórios que possuam configuração prévia na console de gerenciamento.

4.1.1.54. A solução de permitir a geração de relatórios customizáveis e que possam ser exportados para os seguintes formatos, mas não somente:

- PDF;
- CSV.

4.1.1.55. A solução deve permitir a criação de relatórios com as seguintes características:

- Lista com todas as máquinas da rede, gerenciadas ou não;
- Lista de máquinas que estejam com as definições e vacinas de vírus desatualizadas;
- Lista de máquinas com a versão da solução antivírus instalada em cada uma delas;
- Lista com as ameaças de vírus que mais foram encontradas durante as varreduras nas máquinas da rede;
- Lista de máquinas que mais sofreram detecções de vírus em um período determinado;
- Lista de aplicativos com versões desatualizadas nas máquinas da rede;
- Lista de máquinas gerenciadas que possuam seu sistema operacional desatualizado;

4.1.1.56. A solução deve permitir o armazenamento das informações coletadas das estações em um banco de dados centralizado com, no mínimo, as seguintes informações:

- Registro de eventos (LOG);
- Registro de eventos de detecção de vírus e ameaças;
- Registro de status das máquinas da rede;
- Registro de softwares instalados nas máquinas da rede;
- Relatórios de componentes de hardware encontrados em cada máquina da rede.

4.1.1.57. A solução deve ter a capacidade de envio de eventos para um servidor SIEM ou Syslog, suportando, ao menos, os seguintes formatos:

- LEEF;
- JSON;
- CEF.

4.1.1.58. A solução deve fornecer em tempo real o status de conexão de cada máquina da rede, bem como o status atualizado da solução antivírus nas estações de trabalho e servidores.

4.1.1.59. A solução deve permitir a exportação dos relatórios em formato PDF e CSV, para os relatórios que mostrem inventário de hardware e software de todas as estações de rede e servidores ativos na estrutura da console de gerenciamento.

4.1.1.60. A solução deve permitir a instalação do agente e da solução antivírus por meio de GPO e SCCM.

4.1.1.61. A solução deve possuir módulo de gerenciamento para dispositivos móveis com os seguintes sistemas operacionais:

- Android;
- iOS.

4.1.1.62. A console de gerenciamento em nuvem deve permitir o gerenciamento de dispositivos móveis.

4.1.1.63. A solução deve permitir a instalação da solução antivírus nos dispositivos móveis de forma manual com uso de QRCode, ou via link a ser gerado pela console de gerenciamento e enviado por email.

4.1.1.64. A solução deve permitir a ativação da opção do bloqueio de ameaças nas estações de rede e servidores através da console de gerenciamento.

4.1.1.65. A solução deve permitir a configuração de atualização incremental das vacinas de proteção nas estações de rede e servidores.

4.1.1.66. A solução deve permitir a atualização de clientes móveis (Notebooks, laptop, netbook, ultrabooks e similares) a partir do site do fabricante do antimalware, e de outra fonte definida pelo administrador.
4.1.1.67. A solução deve possuir a capacidade de configuração de políticas móveis para computadores que estejam fora da estrutura da organização possam atualizar suas soluções através da internet.

4.1.1.68. A solução deve permitir que as atualizações sejam distribuídas através de comunicação segura entre as estações da rede, o servidor de gerenciamento e o site do fabricante.

4.1.1.69. A solução deve permitir que determinado cliente gerenciado dentro da rede seja eleito como um servidor de distribuição das atualizações, também sendo possível eleger mais de um cliente para essa determinada função.

4.1.1.70. A instalação das atualizações das vacinas deve ser possível sem que haja a necessidade de reinicialização do computador ou dos serviços da solução para que seja possível aplicá-la.

4.1.2. SOLUÇÃO DE ANTIVÍRUS PARA ESTAÇÕES E SERVIDORES

4.1.2.1. A solução deve suportar sistemas operacionais com arquiteturas de 32 e 64 bits;

4.1.2.2. A solução deve ser gerenciada via console de gerenciamento centralizada;

4.1.2.3. A interface do software cliente deve ser fornecida em português Brasileiro;

4.1.2.4. Os manuais da solução devem ser fornecidos em português Brasileiro e inglês;

4.1.2.5. O cliente de instalação das estações de trabalho deve possuir compatibilidade para instalação com os seguintes sistemas operacionais, no mínimo:

- Microsoft Windows 10;
- Microsoft Windows 11;
- Microsoft Windows Server 2012R2;
- Microsoft Windows Server 2016 (Server Core e Desktop Experience);
- Microsoft Windows Server 2019 (Server Core e Desktop Experience);
- Microsoft Windows Server 2022 (Server Core e Desktop Experience);
- Microsoft Windows Server 2025 (Server Core e Desktop Experience);
- Ubuntu Desktop (Versões 20.04LTS, 22.04LTS e 24.04LTS);
- RedHat Enterprise Linux (Versões 8 e 9);
- Linux Mint (Versões 20,21 e 22);
- Ubuntu Server (Versões 20.04LTS, 22.04LTS e 24.04LTS);
- Debian (Versões 11 e 12);
- Alma Linux (Versões 8 e 9);
- Rocky Linux (Versões 8 e 9);
- SUSE Linux Enterprise Server (SLES) 15;
- Oracle Linux (Versões 8 e 9);
- Amazon Linux (Versões 2 e 2023);
- MacOS 11 Big Sur;
- MacOS 12 Monterey;
- MacOS 13 Ventura;
- MacOS 14 Sonoma;
- MacOS 15 Sequoia;
- Android 6 e posteriores;
- iOS 9 e posteriores;

- iPadOS 13 e versões posteriores.

4.1.2.6. O cliente deve possuir a capacidade de manter sua operação mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede, mantendo todas as configurações previamente selecionadas.

4.1.2.7. O cliente deve ter a capacidade de atualizar a versão do agente via console de gerenciamento.

4.1.2.8. Quando o servidor de gerenciamento estiver inoperante ou o agente não conseguir realizar a comunicação com este por razões distintas, o agente deve possuir a capacidade de atualizar as vacinas de proteção e seus componentes através de comunicação com nuvem de dados fornecida pelo fabricante.

4.1.2.9. A solução deve possuir a capacidade de criação de planos para distribuição de atualizações através de comunicação segura entre os clientes e o servidor de gerenciamento.

4.1.2.10. A solução deve permitir o rastreamento de malwares e ameaças de forma agendada, assim como também de forma manual com a possibilidade de selecionar apenas uma máquina ou um grupo de máquinas.

4.1.2.11. O cliente gerenciado deve possuir funcionalidade para bloqueio de ALTERAÇÃO, DESINSTALAÇÃO, DESATIVAÇÃO, IMPORTAÇÃO e EXPORTAÇÃO de suas configurações através de uso de senha configurada no console de gerenciamento para evitar que os usuários das estações de trabalho interfiram no correto funcionamento da solução.

4.1.2.12. A solução deve ser capaz de atualizar as configurações dos clientes sem que haja nenhuma interação com eles (ocorrendo em segundo plano), e sem a necessidade de reinicialização ou logoff.

4.1.2.13. A solução deve possuir a capacidade de bloqueio de ameaças que exploram a ausência de correções no nível do sistema operacional (patches), de forma que essas ameaças sejam bloqueadas enquanto a correção oficial não esteja disponível e instalada corretamente. A solução deve possuir análise heurística e inteligência artificial (Machine Learning) capaz de identificar e bloquear ameaças externas que se utilizem das vulnerabilidades ainda sem uma correção oficial.

4.1.2.14. A solução deve possuir capacidade de análise e bloqueio de arquivos mal-intencionados (Ameaça dia-zero, ameaças persistentes).

4.1.2.15. A solução de escaneamento de vírus e ameaças deverá permitir que sejam configuradas determinadas exclusões:

- Verificação de arquivos com determinadas extensões;
- Arquivos e pastas com caminhos pré-determinados, e com determinado hash.

4.1.2.16. A solução deve permitir a instalação e desinstalação das soluções de proteção de forma remota através da console de gerenciamento.

4.1.2.17. A solução deve permitir a instalação de forma manual através de mídia de instalação fornecida ou gerada através da console de gerenciamento.

4.1.2.18. A solução deve permitir que sejam configuradas as atualizações automáticas das listas de definições de vírus a partir de local pré-definido da rede, com frequência de, no mínimo 1 hora e de acordo com horários previamente definidos na console de gerenciamento e com as seguintes configurações/atualizações:

- Atualização incremental da lista de definições de vírus;
- Atualização por endereço do fabricante como alternativa ao servidor local;
- Configuração remota de ordem de preferência de endereços dos servidores de atualização;
- Configuração do cliente com o servidor de gerenciamento através de serviço de proxy local;
- Atualização de lista de arquivos a serem verificados através da lista de definições de vírus.

4.1.2.19. Para os sistemas operacionais Linux, além da proteção e rastreio do sistema de arquivos contra ameaças, a solução também deve proteger os arquivos contidos em compartilhamentos SAMBA/CIFS e os arquivos que possam estar sendo disponibilizados para acesso de clientes com sistemas operacionais Windows.

4.1.2.20. A solução deve ser capaz de detectar e remover todo e qualquer tipo de malwares, vírus, ramsomware, worm, trojan, spyware, rootkit, exploits, vírus de macro e códigos maliciosos.

4.1.2.21. A solução deve possuir mecanismos de detecção totalmente baseados em ferramentas de análise e detecção, como:

- Machine Learning
- Intrusion Prevent System
- Inteligência Artificial

4.1.2.22. A solução deve possuir rastreamento em tempo real de vírus de macro e novos arquivos criados, copiados, renomeados, movidos ou modificados inclusive em sessões DOS abertas pelo Windows.

4.1.2.23. A solução deve possuir módulo de proteção em tempo real para o sistema de arquivos para detecção de código malicioso quando os arquivos são abertos, editados, criados ou executados.

4.1.2.24. A solução deve possuir módulo de detecção proativa para proteção contra uma nova ameaça assim que a infecção e propagação inicial ocorrer.

4.1.2.25. A solução para estações de trabalho com sistemas operacionais Windows deve possuir módulo com funcionalidade de navegador seguro com proteção de acesso a websites que contenham e trafeguem dados sensíveis e confidenciais. Módulos convencionais de proteção WEB não serão aceitos e deverá existir uma camada adicional de segurança exclusivamente para essa proteção.

4.1.2.26. A solução deve empregar proteção a ameaças baseada em nuvem com conexão direta aos laboratórios de pesquisa e desenvolvimento do fabricante.

4.1.2.27. A solução deve possuir módulo dedicado a detecção e proteção contra ramsomware e suas variantes existentes, a fim de atuar como escudo e proteção deste vetor de ataque.

4.1.2.28. O módulo de detecção e proteção contra ramsomwares deve contar com recurso de remediação (rollback), permitindo que os arquivos criptografados no momento da infecção e propagação sejam restaurados ao seu estado original.

4.1.2.29. O recurso de remediação do módulo de detecção e proteção contra ramsomwares deve ser construído utilizando exclusivamente um motor de Machine Learning de forma a aumentar sobremaneira a eficácia do processo de restauração. Não serão aceitas soluções que utilizam apenas o mecanismo Volume Shadow Copy (VSS) com uso de snapshots, da Microsoft.

4.1.2.30. A solução deve ser capaz de executar varreduras de segurança nas máquinas mesmo quando elas estiverem em estado ocioso, de forma a oferecer proteção proativa mesmo enquanto os equipamentos não estiverem sendo utilizados.

4.1.2.31. A solução deve ser capaz de executar varreduras de segurança em tempo real nas máquinas mesmo quando estiverem em pleno uso pelos usuários para que o produto seja performático mesmo em máquinas com hardware menos poderoso e de baixo desempenho.

4.1.2.32. A solução deve ser capaz de executar varreduras de segurança em tempo real dos processos de memória para a captura de vírus e ameaças que não utilizam arquivos como vetor de ataque.

4.1.2.33. A solução deve efetuar a detecção de tempo real e limpeza de programas maliciosos como spyware, ramsomware, adwares, jokes, discadores, ferramentas de administração remota e softwares quebradores de senha, de forma a removê-los e realizar a restauração das áreas do sistema que tenham sido danificadas por eles, com a possibilidade da criação de uma lista de exclusão de softwares não desejados, de forma que essa administração seja centralizada pela console de gerenciamento.

4.1.2.34. A solução deve possibilitar o rastreamento de ameaças acionado de forma manual com interface gráfica customizável na console de gerenciamento, oferecendo a opção de limpeza após a identificação das ameaças.

4.1.2.35. A solução deve permitir o rastreamento de ameaças acionado através de linha de comando, parametrizável e com opção de limpeza.

4.1.2.36. A solução deve permitir que os rastreios automáticos de malware sejam programados para horários pré-determinados com as seguintes opções:

- Locais de busca: Todos os drives locais, drives específicos e pastas específicas;
- Ações: Somente alertas, limpar automaticamente, apagar automaticamente ou mover automaticamente para a área de segurança.
- Frequência: Diária, semanal e mensal.
- Exclusões: Pastas e arquivos que devem ser excluídos do rastreio

4.1.2.37. A solução deve criar uma área de segurança (Quarentena) nas estações de rede que estiverem executando a proteção antivírus.

4.1.2.38. A solução deve detectar anomalias nos arquivos através dos métodos de assinatura, heurística e por comportamento.

4.1.2.39. A solução deve conter, ao menos as seguintes opções na proteção contra ameaças via internet:
- Ajuste no nível de sensibilidade da detecção;
- Lista de exclusões.

4.1.2.40. A solução deve prover detecção em tempo real e bloqueio de malwares provenientes de downloads realizados no ambiente web e sua remoção.

4.1.2.41. A solução deve permitir que a funcionalidade de rastreamento em tempo real na navegação web possa ser desabilitada pelo administrador a qualquer momento.

4.1.2.42. A solução deve realizar a detecção em tempo real com possibilidade de bloqueio e remoção dos malwares que venham a ser recebidos via conteúdo de email e nos anexos.

4.1.2.43. A solução deve permitir que a funcionalidade de rastreamento em tempo real de email possa ser desabilitada pelo administrador.

4.1.2.44.A solução deve oferecer recurso de controle de dispositivos com a capacidade de controlar a adição/ativação/conexão dos seguintes dispositivos:
- HD externo;
- Pendrive;
- Celulares;
- Tablets;
- CD/DVD;
- Impressora USB;
- Armazenamento Firewire;
- Dispositivo Bluetooth;
- Leitor de cartão inteligente;
- Modem;
- Dispositivo de criação de imagem;
- Porta LPT/COM;
- Dispositivo Portátil.

4.1.2.45. O módulo de controle de dispositivos deve estar disponível para ativação nas estações de trabalho com os sistemas operacionais Windows, macOS e Linux.

4.1.2.46. A solução deve prover ferramenta de firewall bidirecional local no cliente com possibilidade de configuração, ativação e desativação através da console de gerenciamento com o uso de filtros para especificação de:
- Aplicação

- Protocolo
- Endereço IP
- Range de endereços IP
- Rede
- Porta
- Range de portas

4.1.2.47. O módulo de firewall bidirecional local deve tratar tráfego de entrada e saída de forma independente.

4.1.2.48. A solução deve permitir o bloqueio de conexão de dispositivos removíveis.

4.1.2.49. A solução deve gerar registro de todos os eventos de vírus em um arquivo (log).

4.1.2.50. A solução deve possuir módulo de geração de relatórios de, ao menos, os seguintes eventos:
- Eventos de detecção de vírus;
- Status da proteção nos clientes da rede;
- Status dos updates da proteção.

4.1.2.51. A solução deve gerar notificações de eventos de detecção de vírus através de alerta por email.

4.1.2.52. A solução deve gerar relatórios sobre os tipos de vírus encontrados, nome do vírus e se é necessária atualização do sistema operacional.

4.1.2.53. A solução deve possuir controle de acesso a discos removíveis que sejam reconhecidos como dispositivos de armazenamento em massa através de barramento USB e outras interface com as seguintes opções:
- Acesso total;
- Leitura e Escrita;
- Leitura e Execução;
- Apenas Leitura;
- Bloqueio total.

4.1.2.54. A solução deve permitir a criação de exceções nos escaneamentos de arquivos.

4.1.2.55. A solução deve permitir o bloqueio de dispositivos com base nos seguintes critérios:
- Fabricante
- Modelo
- Número de Série

4.1.2.56. A solução deve permitir a proteção contra ameaças que sejam provenientes da internet por meio de sistema de reputação de segurança das URLs acessadas.

4.1.2.57. A solução deve permitir a configuração de portas seguras (HTTPS) para escaneamento e verificação de conexões criptografadas.

4.1.2.58. A solução de firewall deve oferecer suporte aos protocolos TCP e UDP.

4.1.2.59. A solução de firewall deve reconhecer o tráfego DNS, DHCP, DHCP e WINS com opção de filtragem e bloqueio.

4.1.2.60. A solução deve possuir proteção contra ataques de Denial of Service (DoS), port scan, spoofing e botnet.

4.1.2.61. A solução deve permitir a criação de assinaturas personalizadas para detecção de ameaças.

4.1.2.62. A solução deve permitir a criação de novas regras personalizadas dentro do módulo de firewall.

4.1.2.63. A solução deve permitir a criação de regras de firewall diferenciadas por aplicação.

4.1.2.64. A solução deve permitir o bloqueio de ataques que são baseados na exploração de vulnerabilidades.

4.1.2.65. A solução deve possuir integração com navegadores web para prevenção de ataques.

4.1.2.66. A solução deve fornecer proteção contra ataques utilizando mecanismo de reputação online com reporte a console de gerenciamento das informações referentes às ameaças durante a navegação web.

4.1.2.67. A solução deve oferecer proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos.

4.1.2.68. As configurações do antimalware deverão ser realizadas através da mesma console da solução antivírus.

4.1.2.69. A solução deve permitir a criação de lista de exceções de arquivos e diretórios para que não sejam varridos nas execuções em tempo real.

4.1.2.70. A solução deve permitir a verificação das ameaças de forma manual, agendada e em tempo real com detecção das ameaças em nível de kernel do sistema operacional com a possibilidade de detecção de rootkits.

4.1.2.71. A solução deve permitir que nas varreduras agendadas o disparo desse processo ocorra por grupos com intervalos de tempo pré-determinados para redução de impacto de desempenho no ambiente.

4.1.2.72. A solução deve permitir a configuração de ações a serem tomadas no momento da detecção e ocorrências de ameaças, incluindo, mas não somente:

- Reparar;
- Deletar;
- Ignorar.

4.1.2.73. A solução deve permitir que as detecções e reparos de arquivos se estendam também a arquivos que estiverem compactados.

4.1.2.74. A solução deve ser capaz de analisar, detectar e reparar ameaças de vírus em arquivos compactados incluindo, ao menos, 5 níveis de compactação.

4.1.2.75. A solução deve suportar a varredura nos seguintes, mas não somente, padrões de compactação:
- CAB;
- ZIP;
- RAR;
- LHA;
- ARJ;
- TAR.

4.1.2.76. A solução deve ter a capacidade de terminar os processos e serviços que tenham sido acionados pela ameaça no momento da detecção.

4.1.2.77. A solução deve possuir a capacidade de identificar a origem da ameaça e infecção para malwares que utilizam compartilhamento de arquivos como forma de propagação, informando nome e/ou endereço IP da origem com opção de bloqueio de comunicação via rede.

4.1.2.78. A solução deve permitir que a verificação de malwares em recursos mapeados de rede seja bloqueada.

4.1.2.79. A solução deve possuir a capacidade de monitoramento em tempo real através de heurística fazendo o cruzamento e correlacionando com a reputação de arquivos online.

4.1.2.80. Não serão permitidas soluções de verificação de malware que possuam motor de terceiros.

4.1.2.81.A solução deve permitir que o bloqueio de execução de aplicações seja baseado em nome e pasta.

4.1.2.82. A solução deve permitir que a detecção de ameaças desconhecidas na memória seja feita pelo comportamento dos processos e arquivos das aplicações.

4.1.2.83. A solução deve possuir a capacidade de detecção de softwares keyloggers por comportamento dos processos em memória.

4.1.2.84. A solução deve possuir capacidade de detecção de worms e trojans através do comportamento dos processos em memória com opção de alteração dos níveis de sensibilidade da detecção.

4.1.2.85. A solução deve possuir a capacidade de realizar inspeção das ameaças em ambientes isolados utilizando ferramentas, mas não somente, como:
- Aprendizado de máquina
- Deep Learning;
- Análise estatística e dinâmica;

- Detecção baseada em comportamento;
- Introspecção na memória.

4.1.2.86. A solução deve ter a capacidade de realizar a detecção do malware através do DNA do vírus encontrado.

4.1.2.87. A solução deve ter a capacidade de identificar e atualizar os patches do sistema operacional.

4.1.2.88. A solução deve ter a capacidade de identificar o uso do hyper-v e possuir uma verificação de malware específica para esse hypervisor.

4.1.2.89. A solução deve possuir a capacidade de realizar escaneamentos em estações que utilizam One Drive for Business, procurando por ameaças, vírus e arquivos comprometidos ou possíveis malwares que possam ter sido armazenados nessa nuvem.

4.1.2.90. A solução de proteção de servidor deve possuir a capacidade de adicionar ameaças com comportamento malicioso a uma lista negra.

4.1.2.91. A solução deve ser capaz de adicionar exclusões automáticas para aplicativos de servidor de alta criticidade.

4.1.2.92. A solução deve possuir a capacidade de otimização de desempenho para infraestruturas híbridas (Física e virtual) com a eliminação da duplicação de verificação de arquivos, automaticamente excluindo a varredura para arquivos que já tenham sido verificados e limpos.

4.1.2.93. A solução deve possuir módulo para controle de acesso de redes com possibilidade de bloqueio dos acessos.

4.1.2.94. A solução deve permitir a criação de políticas de bloqueio com base em categorias e listas de URL.

4.1.2.95. A solução deve permitir a geração de relatórios de sites que tenham sido acessados e bloqueados.

4.1.2.96. A solução deve permitir a personalização das mensagens exibidas quando um site for bloqueado.

4.1.2.97. A solução deve possuir recurso para verificação de malwares nas mensagens de email pelo antimalware instalado nas estações de trabalho, suportando os seguintes, mas não somente, protocolos de email:

- POP3;
- POP3S;
- IMAP;
- IMAPS.

4.1.2.98. A solução deve permitir a criação e configuração de ações personalizadas para detecções realizadas pelo módulo de proteção de email suportando, mas não somente, as seguintes ações:

- Mover email para pasta específica;

- Excluir o email;
- Manter o email.

4.1.2.99. Em equipamentos macOS a solução deve possuir módulo de proteção para emails enviados e recebidos.

4.1.2.100. A solução deve possuir módulo de anti-phishing para proteção dos usuários que acessam sites web falsos para obtenção de dados e informações sensíveis e confidenciais.

4.1.2.101. A solução de proteção AntiSpam deve fazer as verificações utilizando o protocolo SSL.

4.1.2.102. O módulo de proteção anti-spam deve ser nativo e totalmente integrado ao endpoint.

4.1.2.103. A solução deve possuir protocolo de replicação com protocolo HTTPS e serviço de notificação via push e/ou webhook.

4.1.3 SOLUÇÃO DE SANDBOX EM NUVEM

4.1.3.1. A solução deve pertencer ao mesmo fabricante e estar totalmente integrada com a solução de proteção de endpoints, permitindo o gerenciamento através da console.

4.1.3.2. A solução deve estar disponível para integração com os sistemas operacionais Windows, Linux e macOS para estações de rede e servidores.

4.1.3.3. A solução deve estar disponível e totalmente integrada com a console de gerenciamento em nuvem.

4.1.3.4. A análise inicial de artefatos deve ocorrer de forma local na própria solução de endpoint, e o envio destes artefatos para a solução de verificação em sandbox deve acontecer de forma automática sem intervenção dos usuários.

4.1.3.5. A solução deve permitir o envio manual de artefatos para verificação no sandbox em nuvem através da interface do endpoint, permitindo assim que os usuários e administradores possam confirmar se determinados artefatos representam perigo para o usuário, para o ambiente e a rede como um todo.

4.1.3.6. A solução deve apresentar todos os artefatos enviados para o sandbox através da console de gerenciamento juntamente com o resultado da análise, permitindo que o administrador tenha visibilidade de todos os artefatos que foram escaneados, limpos e removidos pelo módulo de sandbox.

4.1.3.7. A solução deve gerar relatório de comportamento para cada artefato enviado e processado pela solução de sandbox.

4.1.3.8. A solução deve permitir que os relatórios dos artefatos enviados para a solução de sandbox sejam exportados para os formatos JSON e PDF.

4.1.3.9. O relatório de comportamento dos artefatos gerado pela solução de sandbox deve exibir, mas não somente, as seguintes informações sobre o artefato analisado:

- Resultado da análise;
- Detalhes do arquivo verificado;
- HASH SHA-1;
- HASH SHA-256;
- Detalhes da análise do arquivo.

4.1.3.10. Caso a solução de sandbox estiver em uso concorrente com a solução de detecção e resposta a ameaças, deve possuir a capacidade de fornecer informações adicionais sobre o arquivo analisado, exibindo, mas não somente, as seguintes informações:

- Comportamentos analisados;
- Ações realizadas em processos;
- Arquivos afetados;
- Registros afetados;
- Chamadas de API;
- Atividade de rede;
- Outros eventos;
- Análise estatística;
- Detalhes do artefato;
- Geometria do arquivo;
- Importações de bibliotecas;
- Funções de exportação de arquivos .dll;
- Métodos e funções utilizados pelo artefato.

4.1.3.11. A solução deve permitir que sejam criadas exclusões por caminho, nome da detecção, extensão e HASH SHA-1 do arquivo.

4.1.3.12. A solução deve permitir que sejam criadas configurações a nível granular para o envio automático de amostras para o módulo de sandbox com a permissão de habilitar e desabilitar, mas não somente, o envio das categorias de arquivos:

- Executáveis;
- Arquivos;
- Scripts;
- Documentos.

4.1.3.13. A solução deve possuir recurso de configuração para definição de tempo máximo que os artefatos estarão disponíveis nos servidores do módulo de sandbox.

4.1.3.14. A solução deve permitir a definição de tamanho máximo dos arquivos (em MB) para análise automática de artefatos no módulo de sandbox.

4.1.3.15. A solução deve permitir a configuração do tamanho máximo do arquivo a ser enviado para análise no módulo de sandbox.

4.1.3.16. A solução deve exibir um aviso no momento do envio pela primeira vez de um arquivo considerado suspeito. Se a verificação for concluída antes da execução do arquivo o aviso não deverá ser exibido, e a solução deve eliminar automaticamente as amostras dos arquivos e executáveis nos servidores onde o comportamento foi analisado.

4.1.3.17. A solução de sandbox deve ter a capacidade de envio de emails de SPAM para análise.

4.1.3.18. A solução de sandbox deve classificar os artefatos em determinadas categorias, mas não somente:
- Desconhecido;
- Limpo;
- Suspeito;
- Altamente suspeito;
- Malicioso.

4.1.3.19. A solução deve disponibilizar as seguintes informações de um arquivo enviado para análise em sandbox:
- Nome da estação que enviou o arquivo;
- Usuário conectado ao dispositivo;
- Resultado da análise;
- HASH SHA-1;
- Nome do arquivo;
- Tamanho do arquivo;
- Categoria.

4.1.3.20. A solução deve oferecer proteção proativa para que os arquivos/executáveis analisados sejam bloqueados até que o resultado da análise de sandbox esteja disponível.

4.1.3.21. A solução deve possuir integração total com a solução de anti-malware para criação e aplicação de políticas.

4.1.4. SOLUÇÃO PARA CRIPTOGRAFIA DE DISCOS

4.1.4.1. A solução deve ser capaz de criptografar dispositivos que utilizem sistemas operacionais Windows e macOS.

4.1.4.2. Nas estações com sistema operacional Windows a solução deverá possuir tecnologia proprietária de criptografia. Não serão aceitas soluções que apenas gerenciem e/ou façam uso do motor de criptografia Microsoft BitLocker.

4.1.4.3. Para estações com sistema operacional macOS a solução deve ser capaz de gerenciar o FileVault da Apple.

4.1.4.4. A solução deve dispor de recurso que permita aos administradores terem visibilidade de quais dispositivos da rede possuem o módulo de criptografia instalado e os que ainda não possuem.

4.1.4.5. A solução deve permitir que os administradores tenham visibilidade dos dispositivos criptografados e sua aderência às políticas de criptografia definidas e os dispositivos sem criptografia aplicada e possíveis problemas ocorridos no momento da criptografia.

4.1.4.6. A solução deve ser capaz de criptografar os dispositivos desejados desde a inicialização do sistema operacional.

4.1.4.7. A solução deve fornecer possibilidades de recuperação de senha para usuários remotos que se encontrem bloqueados.

4.1.4.8. A solução deve possuir a capacidade de programação das tarefas de criptografia para os dispositivos desejados com a possibilidade de retomar a execução desde seu último estado em caso de pausa da tarefa.

4.1.4.9. A solução deve ser administrada através da console de gerenciamento juntamente com as outras soluções descritas neste documento.

4.1.4.10. A solução deve possuir recurso para criptografar e descriptografar apenas o espaço em disco utilizado.

4.1.4.11. A solução deve possuir a opção de criptografia apenas do disco sendo utilizado para inicialização, e todos os discos.

4.1.4.12. A solução deve possuir opções para utilização de TPM (Trusted Platform Module) se disponível, e forçar a utilização de TPM para aplicação da criptografia.

4.1.4.13. A solução deve possuir compatibilidade com a tecnologia de auto criptografia OPAL.

4.1.4.14. Se a tecnologia OPAL estiver disponível, a solução deve forçar o uso desta para aplicação da criptografia de disco.

4.1.4.15. A solução deve suportar e ter compatibilidade com o uso de Single Sign-on (SSO), permitindo que o usuário realize apenas uma autenticação em seu dispositivo. No momento da autenticação da solução o usuário não deverá inserir suas credenciais novamente e ser logado automaticamente no sistema operacional.

4.1.4.16. A solução deve permitir que o administrador possa configurar os requerimentos mínimos de definição de senha utilizada na criptografia, com os seguintes, mas não somente, parâmetros:

4.1.4.17. Alteração de senha sem intervenção do administrador, através da interface da solução;

4.1.4.18. Caracteres da senha:
- Utilização de caracteres em caixa alta;
- Utilização de caracteres em caixa baixa;
- Utilização de números;
- Comprimento mínimo de senha.

4.1.4.19. Tempo de expiração da senha;

4.1.4.20. Configuração de limite de tentativas incorretas de utilização da senha de criptografia;

4.1.4.21. Configuração de limite máximo de tentativas incorretas de utilização da senha de criptografia.

4.1.4.22. Expiração da senha:
- Configuração de expiração da senha utilizada na criptografia;
- Tempo de expiração da senha (dias)

4.1.4.23. A solução deve ter a capacidade de envio de alerta ao usuário com informações sobre a expiração da senha, caso essa configuração esteja habilitada.

4.1.4.24. A solução deve permitir que o administrador defina a quantidade de dias de antecedência para o alerta de expiração de senha ser enviado ao usuário.

4.1.4.25. A solução deve permitir que o administrador instale a solução com uma senha pré-definida sem a necessidade de o usuário criar uma senha para a criptografia.

4.1.4.26. A solução deve permitir que seja possível desativar a senha de login do usuário, através da console de gerenciamento e solicitar que esta seja alterada via interface gráfica.

4.1.4.27. A solução deve permitir o bloqueio da senha de login do usuário, permitindo que ele faça o acesso através da senha única de recuperação, a ser gerada via console de gerenciamento.

4.1.4.28. A solução deve ter a capacidade de remoção da senha de login do usuário, para que a máquina possa ser iniciada somente via ferramenta de recuperação avançada que será executada pelos administradores da solução na rede. Caso o dispositivo estiver em uso durante no momento da ação de remoção, este deve ser reinicializado automaticamente para garantir o sucesso da ação.

4.1.4.29. A solução deve permitir que o administrador faça a desativação temporária da tela de autenticação através da console de gerenciamento, para realização de manutenções nos equipamentos sem que a senha de criptografia seja solicitada e possa reativá-la automaticamente após a conclusão da manutenção.

4.1.4.30. A solução deve permitir a desativação permanente da tela de autenticação, quando necessário.

4.1.4.31. A solução deve possibilitar que o administrador recupere os dados caso o usuário não consiga acessar a máquina com suas credenciais.

4.1.4.32. A senha de recuperação gerada pela solução deve ser única para cada máquina.

4.1.4.33. A solução deve possibilitar que o administrador gere uma nova senha de recuperação para o dispositivo.

4.1.4.34. A solução deve prover ferramenta de recuperação avançada, para casos em que exista a impossibilidade de inicialização correta do dispositivo por falha física ou de sistema operacional. Essa ferramenta deve permitir a inicialização da máquina através de mídia (Pendrive, USB e DVD) permitindo que os dados sejam recuperados após a descriptografia manual do disco.

4.1.4.35. A solução deve possuir compatibilidade com a tecnologia Microsoft Direct Storage.

4.1.4.36. A solução deve possuir compatibilidade com tecnologia AES-NI que utiliza o conjunto de instruções dos algoritmos Advanced Encryption Standard (AES) que torna o processo de criptografia e descriptografia mais rápido e eficiente.

4.1.5. REQUERIMENTOS GERAIS

4.1.5.1. A solução ofertada não deve possuir restrições sobre a quantidade de equipamentos por sistemas operacionais para ativação de suas licenças. A totalidade do número de licenças contratadas deve ser ativada completamente em servidores, estações de trabalho e dispositivos móveis, respeitando apenas o limite total contratado.

4.1.5.2. Todos os módulos ofertados pelo fabricante devem ser ativados com a utilização de uma única licença sem a necessidade de aquisição de módulos separados (Addons)

4.2. SUPORTE TÉCNICO E MONITORAMENTO

4.2.1. O suporte técnico deve ser prestado pela fornecedora da solução, cobrindo toda solução de antivírus contratada e não será aceito subcontratação.

4.3. CHAMADOS E ATENDIMENTO TÉCNICO

4.3.1. A CONTRATANTE deve poder abrir chamados de manutenção através de chamada telefônica para número, central de atendimento via navegador (Web) ou correio eletrônico, sem a necessidade prévia de consulta e/ou qualquer liberação por parte da fornecedora da solução.

4.3.2. O atendimento técnico remoto deverá ocorrer de segunda a sexta-feira (exceto feriados), das 09h00 às 18h00.

4.3.3. O contrato de suporte técnico deverá ser de 36 meses (três anos).

4.3.4. Não deve haver limites para aberturas de chamados ou limite de tempo de atendimento, sejam dúvidas, configurações ou resolução de problemas.

4.3.5. A equipe de suporte técnico deverá buscar, no escopo de serviços, prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes correlacionando-os e identificando a causa-raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos.

4.3.6. A fornecedora da solução deve realizar atendimentos remotos à equipe de Tecnologia da Informação da CONTRATANTE, a partir de solicitações recebidas dos analistas ou do gestor do processo, via sistema de atendimento, telefone ou correio eletrônico.

4.3.7. Todos os atendimentos deverão estar registrados em central de atendimento técnico e gestão de chamados.

4.3.8. Deve haver realização de otimizações nas configurações para melhor do desempenho, quando observadas quedas de desempenho ou indisponibilidades pela CONTRATANTE.

4.3.9. A fornecedora da solução deve garantir que os profissionais designados para atendimento técnico são capacitados para tanto.

4.3.10. A CONTRATADA não será responsável pelo atendimento em sistemas operacionais defasados ou descontinuados pelo fabricante.

4.3.11. Garantia de tempo de resposta e nível de serviço:

4.3.12. A garantia de tempo de resposta será realizada conforme critérios de prioridades a seguir:

Classe	Descrição	Início do atendimento em até:
1	Serviço indisponível.	2 horas
2	Suporte técnico de maior impacto.	4 horas
3	Suporte técnico com menor impacto.	8 horas
4	Manutenção preventiva.	Programada

4.3.13. O acordo de nível de serviço para suporte técnico deverá obedecer ao seguinte escopo:

Prioridade	Descrição
1 (Emergencial)	O serviço está fora de operação ou há um impacto crítico nas operações dos negócios.

2 (Alta)	O serviço está degradado, ou aspectos significativos das operações de negócio sofreram impactos negativos pelo desempenho inadequado.
3 (Média)	Serviço funcionando com pequenos problemas sem impacto direto na operação.
4 (Baixa)	O desempenho operacional do serviço está prejudicado, não causando quebra de funcionamento ou de operação.

4.3.14. As horas para primeiro atendimento e resolução de incidentes são horas corridas e serão contabilizadas dentro do horário de atendimento descrito neste termo de referência.

4.3.15. A CONTRATADA deverá disponibilizar e gerenciar os atendimentos técnicos da CONTRATANTE através de portal de gerenciamento de atendimentos com acesso através de navegador web.

4.3.16. Mesmo os chamados sendo abertos através de ligação telefônica ou correio eletrônico, os chamados deverão ser registrados na central.

4.3.17. A solução deverá ser aderente aos processos do ITIL para gerenciamento de incidentes e requisições.

4.3.18. A CONTRATADA deverá emitir relatórios mensais abrangendo, no mínimo, requisições, incidentes, informações de atendimentos e soluções conforme linha de atendimento com especificações e detalhes de cada atendimento.

4.3.19. A CONTRATANTE deverá ser avisada através de e-mail sobre a abertura e solução de qualquer tipo de solicitação através do portal WEB, telefone e e-mail.

4.3.20. O sistema operacional e servidor responsável por suportar a console de gerenciamento de atendimentos e informações fica sob responsabilidade da CONTRATADA, sendo essa responsável por sua atualização e manutenção.

4.3.21. A solução deverá conter a possibilidade de criação de regras de negócio, para automação no atendimento técnico especializado.

4.3.22. O sistema de gerenciamento de chamados deverá ter histórico de alterações do chamado bem como solução, para eventuais processos de auditoria.

4.3.23.A CONTRATADA deverá garantir que a solução de atendimento e informações conte com uma área de cadastro de contatos, para consulta pela CONTRATANTE.

4.3.24. Deverá ser possível anexar documentos de qualquer tipo na abertura e gerenciamento de atendimentos técnicos.

4.3.25. Os atendimentos técnicos deverão ser organizados por categoria, que serão acordados junto a CONTRATANTE.

4.3.26. O sistema de atendimento deverá contar com a função de aprovação dos atendimentos técnicos, sendo possível o envio de tal aprovação para gestores e responsáveis pelos devidos atendimentos junto a CONTRATANTE.

4.3.27. Deverá ser possível o envio de notificação de abertura e solução de atendimentos para um grupo de e-mails.

4.3.28. A solução de atendimento técnico deverá permitir que o chamado possa ser exportado para o formato ".PDF".

4.3.29. A solução deverá contar com perfis de usuários, sendo possível a criação de acessos somente leitura.

4.3.30. Deverá ser possível a criação de grupos de usuários na solução.

4.3.31. A solução disponibilizada pela CONTRATADA deverá ter a possibilidade da criação de várias entidades dentro de um mesmo banco de dados da solução.

- Relatórios Mensais, durante o período do contrato
- Relatório de Chamados:
- Categoria do chamado;
- Usuário;
- Ativos relacionados;
- Data de abertura e fechamento;
- Status;

4.3.32. O suporte técnico deverá ter os seguintes canais de atendimento: Suporte Telefônico, E-mail e Sistema online de chamados, todos em português do Brasil.

4.3.33. A CONTRATADA deverá sempre disponibilizar versões mais recentes dos softwares sem ônus financeiro.

5. REQUISITOS DA CONTRATAÇÃO

5.1. Sustentabilidade: Os critérios de sustentabilidade estão eventualmente inseridos na descrição do objeto.

5.2. Subcontratação: Não é admitida a subcontratação do objeto contratual.

5.3. Garantia da contratação: Não haverá exigência da garantia da contratação do art. 96 e seguintes da Lei nº 14.133/21, a fim ampliar a competitividade.

6. FORMA DE EXECUÇÃO DO OBJETO

6.1. Do prazo, do local e das condições de prestação dos serviços

6.1.1 O prazo para entrega do objeto será de até 10 (dez) dias úteis, contados do recebimento do Pedido de Compra.

6.1.2. O pedido será emitido pelo Setor de Compras.

6.1.3. Os serviços serão prestados na Sede da Câmara Municipal de Carapicuíba/SP, localizada na Travessa Virginio Pasini, 63 – Jardim São Pedro, Carapicuíba – SP , CEP: 06320-000.

6.1.4. As despesas de custeio com deslocamento, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos, ficam a cargo exclusivo da Contratada;

6.2. Obrigações do Contratante:

6.2.1. Receber, acompanhar, fiscalizar, conferir e avaliar o objeto do contrato afim de que sejam executados rigorosamente em conformidade com o estabelecido no processo de contratação;

6.2.2. A fiscalização do contrato, por parte do Contratante, não exonera nem diminui a completa responsabilidade da Contratada por inobservância ou omissão a qualquer das cláusulas contratuais estabelecidas no ajuste;

6.2.3. Notificar a Contratada de qualquer irregularidade constatada, por escrito para que seja sanada;

6.2.4. Efetuar o pagamento nas condições e nos preços pactuados em contrato.

6.2.5. Aplicar à contratada as penalidades regulamentares e contratuais.

6.3. Obrigações da Contratada:

6.3.1. Fornecer o objeto em estrita conformidade com as especificações e condições estabelecidas no Processo Administrativo nº 3189/2025, Dispensa de Licitação nº 34/2025, termo de referência, proposta apresentada e demais condições estabelecidas em contrato;

6.3.2. Manter-se em compatibilidade com as obrigações assumidas no contrato durante toda a sua execução, conservando todas as condições de habilitação e qualificação exigidas na contratação;

6.3.3. Designar preposto para representar a Contratada na execução do contrato.

6.3.4. Prestar todos os esclarecimentos que forem solicitados pela Câmara Municipal, obrigando-se a atender, de imediato, todas as reclamações a respeito dos serviços prestados.

6.3.5. Responsabilizar-se por quaisquer prejuízos que causar à Contratante em decorrência do não cumprimento ou cumprimento irregular das obrigações assumidas;

6.3.6. Arcar com o pagamento de quaisquer tributos, multas ou ônus oriundos da contratação, pelos quais seja responsável, principalmente os de natureza fiscal e comercial;

6.3.7. Atender prontamente às notificações, reclamações, exigências ou observações feitas pela Contratante, refazendo ou corrigindo, quando for o caso, às suas expensas, o objeto que eventualmente tenha sido executado em desacordo com o combinado;

6.3.8. Não transferir, no todo ou em parte, o presente contrato;

6.3.9. Cumprir outras obrigações previstas no Código de Proteção e Defesa do Consumidor (Lei Federal nº 8.078, de 11 de setembro de 1990) que sejam compatíveis com o regime de direito público.

6.4. Da vigência do contrato

6.4.1. O Contrato terá vigência de 36 (trinta e seis).

7. GESTÃO DO CONTRATO

7.1. Os gestores e fiscais de contratos e os respectivos substitutos serão representantes da Câmara Municipal de Carapicuíba/SP designados pela autoridade competente, com atribuições de acompanhar e fiscalizar a execução do contrato, nos termos dos art. 21 a 23, observados os requisitos estabelecidos no art. 11, do Ato da Mesa nº 7/2024, de 11 de dezembro de 2023, que regulamenta a Lei nº 14.133, de 1º de abril de 2021, no âmbito da Câmara Municipal de Carapicuíba.

7.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade ou ainda resultante de imperfeições técnicas, vícios redibitórios, não implica em corresponsabilidade do Contratante ou de seus agentes e prepostos.

8. CRITÉRIOS PARA MEDIÇÃO E PAGAMENTO

8.1. Do recebimento dos serviços

8.1.1. O recebimento do objeto do contrato ocorrerá da seguinte forma:

8.1.1.1. **Provisoriamente**, pelo responsável por seu acompanhamento e fiscalização, mediante termo detalhado, quando verificado o cumprimento das exigências de caráter técnico previamente definidos no contrato;

8.1.1.2. **Definitivamente**, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais.

8.1.2. Os prazos e os métodos para a realização dos recebimentos provisório e definitivo deverão ser definidos no contrato.

8.2. Do prazo e forma de pagamento

8.2.1. O pagamento será realizado no prazo máximo de até 5 (cinco) dias, contados a partir do recebimento da Nota Fiscal/Fatura devidamente atestada pela competente área, por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pela Contratada, ou através de boleto bancário com vencimento mínimo de 5 (cinco) dias.

8.2.2. Constatando-se alguma irregularidade da Contratada, será providenciada sua notificação, por escrito, para que, no prazo de 05 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Administração Contratante.

8.2.3. Não será iniciada a contagem de prazo caso os documentos fiscais apresentados ou outros necessários contenham incorreções.

8.2.4. Quando for constatada qualquer irregularidade na nota fiscal, a Contratante solicitará imediatamente a Contratada carta de correção, quando couber, ou ainda a pertinente regularização, que deverá ser encaminhada à Contabilidade da Câmara Municipal de Carapicuíba, no prazo de 3 (três) dias úteis.

8.2.5. Caso a Contratada não apresente carta de correção no prazo estipulado, o prazo para pagamento será reiniciado a partir da data da sua apresentação.

8.2.6. Todo e qualquer pagamento será efetuado direta e exclusivamente à Contratada, eximindo-se a Contratante de obrigações a terceiros por títulos colocados em cobrança, descontos, caução ou outra modalidade de circulação ou garantia, inclusive quanto a direitos emergentes desta, ficando estabelecido que, em hipótese alguma, aceitará tais títulos, os quais serão devolvidos, incontinente, à pessoa física ou jurídica que os houver apresentado.

8.2.7. Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação financeira de penalidade que lhe tenha sido imposta.

8.2.8. A Câmara Municipal de Carapicuíba não se responsabilizará por quaisquer autuações fiscais e gravames futuros decorrentes de interpretações errôneas por parte do licitante vencedor quanto à aplicação de tributos e suas alíquotas, suspensões, base de cálculo, isenções etc.

8.3. Do critério de reajuste/repactuação

8.3.1. O critério de reajuste será definido no instrumento de contrato.

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

9.1. Forma de seleção e critério de julgamento da proposta

9.1.1. O fornecedor será selecionado por meio da realização de procedimento de DISPENSA DE LICITAÇÃO, com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL, nos Termos do

art. nº 75, Inciso II da Lei 14.133/2021 e do Ato da Mesa nº 7/2023.

9.2. Exigências de habilitação

9.2.1. Para fins de habilitação, deverá o fornecedor comprovar os seguintes requisitos mínimos, conforme artigo 62 e 14 da Lei Federal 14.133/2021:

9.2.1.1. Habilitação Jurídica

9.2.1.1.1. Registro comercial, no caso de empresa individual;

9.2.1.1.2. Ato constitutivo, estatuto social, contrato social ou sua consolidação e posteriores alterações contratuais, devidamente registradas na junta comercial e, em vigor; e no caso de sociedade por ações, acompanhado da ata de eleição de sua atual administração, registrados e publicados;

9.2.1.1.3. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova da diretoria em exercício;

9.2.1.1.4. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

9.2.1.1.5. Em se tratando de Microempreendedor Individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br

9.2.1.2. Regularidade fiscal, social e trabalhista

9.2.1.2.1. Prova de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);

9.2.1.2.2. Regularidade perante a Fazenda Municipal;

9.2.1.2.3. Regularidade perante a Fazenda Estadual;

9.2.1.2.4. Regularidade perante a Fazenda Federal;

9.2.1.2.5. Regularidade perante o FGTS;

9.2.1.2.6. Regularidade perante a Justiça do Trabalho;

9.2.1.3. Qualificação Econômico-financeira

9.2.1.3.1. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II).

9.2.1.4. Outras comprovações

9.2.1.4.1. Consulta ao Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS;

9.2.1.4.2. Consulta ao Cadastro de Apenados do Tribunal de Contas Estado de São Paulo;

9.2.1.4.3. Consulta ao Cadastro de Licitantes Inidóneos do Tribunal de Contas da União;

9.2.1.4.4. Declaração conjunta, conforme modelo Anexo II deste Termo;

9.2.1.4.5. Serão aceitas certidões positivas com efeito de negativas.

9.2.1.10. Caso o fornecedor seja considerado isento dos tributos municipais relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei;

10. INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

10.1. Comete infração administrativa, nos termos do art. 155 da Lei nº 14.133/2021, o fornecedor que:

10.1.1. Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade da proposta;

10.1.2. Apresentar declaração ou documentação falsa exigida para a dispensa ou prestar declaração falsa durante o processo de contratação;

10.1.3 Deixar de entregar a documentação exigida para a dispensa;

10.1.4. Não mantiver a proposta, salvo em decorrência de fato superveniente devidamente justificado;

10.1.5. Fraudar a dispensa;

10.1.6. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

10.1.7. Praticar atos ilícitos com vistas a frustrar os objetivos da dispensa;

10.1.8. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

10.2. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções previstas no art. 156 da Lei nº 14.133, de 2021:

10.2.1. Advertência;

10.2.2. Multa de 0,5% a 30% (cinco décimos por cento a trinta por cento) sobre o valor estimado da contratação;

10.2.3. Impedimento de licitar e de contratar, pelo prazo de até 03 (três) anos, nos termos do artigo 156, inciso III, combinado com o § 4º, da Lei nº 14.133/2021;

10.2.4. Declaração de inidoneidade para licitar ou contratar, pelo prazo mínimo de 03 (três) anos e máximo de 06 (seis) anos, nos termos do artigo 156, inciso IV, combinado com o § 5º, da Lei Licitatória.

10.3. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

10.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 14.133, de 2021, e subsidiariamente na Lei nº 9.784, de 1999.

10.5. A autoridade competente, na aplicação das sanções, levará em consideração a natureza e gravidade da infração cometida, as peculiaridades do caso concreto, as circunstâncias agravantes ou atenuantes e os danos que dela provierem para a Administração Pública;
10.6. As importâncias relativas às multas serão descontadas, sempre que possível, do pagamento a que tiver direito a Contratada, ou cobradas judicialmente, se for o caso.

10.7. As sanções por atos praticados no decorrer da contratação serão definidas no instrumento de contrato.

11. ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS

11.1. O custo estimado da contratação é de R$ 29.824,17 (Vinte e nove mil, oitocentos e vinte e quatro reais e dezessete centavos), valor baseado no Estudo Técnico Preliminar.

12. RECURSO ORÇAMENTÁRIO

12.1. 3.3.90.40 – Serviços de Tecnologia da Informação e Comunicação.

13. ANEXO

13.1. Anexo I – Modelo de Proposta Comercial;

13.2. Anexo II – Declaração Conjunta;

13.3. Anexo III – Minuta de Contrato.

14. RESPONSÁVEL PELA ELABORAÇÃO

14.1. Servidores Edson Charles de Lima - Setor de Compras

ANEXO I

MODELO DE PROPOSTA DE PREÇOS

PAPEL TIMBRADO DA EMPRESA

À CÂMARA MUNICIPAL DE CARAPICUÍBA

DISPENSA DE LICITAÇÃO Nº __/2025

PROCESSO Nº __/2025

OBJETO: 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.

DADOS DA EMPRESA	
Razão Social:	
Endereço:	
Município:	CEP:
Contato:	Fone:
E-mail:	
CNPJ:	Inscrição:

Segue nossa proposta para o fornecimento dos itens a seguir:

ITEM	**DESCRIÇÃO**	**PERIODO**	**QTD**	**TIPO**	**VALOR UNIT. R$**	**VALOR TOTAL R$**
1.	**Licenciamento e Serviços**					
1.1.	**Renovação** da solução de antivírus ESET PROTECT Advanced.	36 meses	75	Licenciamento		
1.2.	**Serviço** de suporte técnico, atendimento 8x5 (oito horas por dia, cinco dias por semana), console de gerenciamento em nuvem e monitoramento 24x7 (tempo integral)	36 meses	01	Serviço		
VALOR TOTAL DA PROPOSTA R$						
POR EXTENSO:						

Validade da Proposta: Mínima de 90 (noventa) dias.

Prazo de entrega: De até 10 (dez) dias;

Condições de pagamento: Em até 5 (cinco) dias, após entrega e aprovação.

Local, _____ de _____ de 2026.

_____

Assinatura
Nome, RG, CPF e Cargo

ANEXO II

MODELO DE DECLARAÇÃO CONJUNTA

PAPEL TIMBRADO DA EMPRESA

À CÂMARA MUNICIPAL DE CARAPICUÍBA

DISPENSA DE LICITAÇÃO Nº __/2025

PROCESSO Nº __/2025

OBJETO: 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.

A empresa (Razão Social da Empresa), estabelecida a Rua _____, nº _____, bairro _____, no município de _____, Estado de _____, inscrita no CNPJ/MF sob nº _____, neste ato representada por seu sócio(a)/procurador(a), Sr(a). _____, portador(a) da Cédula de Identidade RG nº _____, inscrito no CPF/MF sob o nº _____, no uso de suas atribuições legais, DECLARA, sob as penas da Lei, que:

a) Que está ciente e, concorda com as condições contidas neste processo de dispensa e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

b) Está sob o regime de microempresa ou empresa de pequeno porte, para efeito do disposto na Lei Complementar 123/2006**. SIM ( ) NÃO ( ).**

Nos termos de legislação vigente, não possuindo nenhum dos impedimentos previstos no § 4º do artigo 3º da lei Complementar nº 123/2006 e suas alterações.

Declaro ainda que, nos termos do artigo 4º, § 2º, da Lei 14.133/2021, não possuo contratos com a Administração Pública que extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

c) Não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos, salvo menor a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição e no inciso VI, do art. 68, da Lei 14.133, de 1º de abril de 2021, acrescido pela Lei nº 9.854, de 27 de outubro de 1999;

d) Não possuí empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

e) Cumpre as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz, conforme orientado pelo art. 92, inciso XVII da Lei 14.133, de 1º de abril de 2021;

f) Não está impedida de participar de licitações ou contratar com a Administração Pública de Carapicuíba e que não é declarada inidônea pelo Poder Público, de quaisquer esferas da Federação. Não se encontra, nos termos da legislação em vigor, sujeito a qualquer outro fato ou circunstância que possa impedir a sua regular participação no presente certame ou a eventual contratação que deste procedimento possa ocorrer, para fins do disposto artigo 156, inc. IV, da Lei nº 14.133/21, 1º de abril de 2021.

g) Não possui sócio ou administrador servidor ou com parentesco até terceiro grau, de servidores e/ou dirigentes desta entidade, que impeçam a contratação desta empresa, nos termos das legislações vigentes aplicáveis;

h) Está ciente de que a falsidade na declaração de que trata os itens anteriores sujeitará a empresa às sanções previstas na Lei n° 14.133, de 2021, e neste Edital;

i) É responsável pela fidelidade e legitimidades das informações e documentos apresentados digitalmente no sistema eletrônico ou presencialmente, estando ciente de que a falsidade de qualquer documento ou a inverdade nele contida ficará sujeita às sanções administrativas e judiciais cabíveis.

Local, _____ de _____ de 2026.

_____

Assinatura
Nome, RG, CPF e Cargo

ANEXO III

MINUTA DE CONTRATO Nº....

DISPENSA DE LICITAÇÃO Nº __/2025

PROCESSO Nº __/2025

CONTRATO QUE CELEBRAM ENTRE SI A CÂMARA MUNICIPAL DE CARAPICUÍBA E A EMPRESA ....

Por este instrumento de contrato e na melhor forma de direito, que entre si celebram, de um lado a **CÂMARA MUNICIPAL DE CARAPICUÍBA**, inscrita no CNPJ sob o nº 49.759.954/0001-71, estabelecida na Travessa Virgínio Pasini, 63, na cidade de Carapicuíba, Estado de São Paulo, neste ato representada por seu **PRESIDENTE RONALDO DE SOUZA,** brasileiro e residente neste Município, doravante denominada simplesmente **CONTRATANTE** e de outro lado a empresa _____, CNPJ nº _____, com sede na _____, neste ato representada por seu _____, Sr.(a) _____, CPF nº ____ e do RG nº _____, doravante denominada **CONTRATADA**, de acordo com o que consta do Processo Administrativo n° __/2025, relativo a Dispensa de Licitação nº __/2025, firmam o presente contrato, mediante condições a seguir:

CLÁUSULA PRIMEIRA – OBJETO

1.1. 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.

CLÁUSULA SEGUNDA - DOS DOCUMENTOS INTEGRANTES DO CONTRATO

2.1. Integram e completam o presente contrato, para todos os fins de efeito e de direito, obrigando as partes em todos os seus termos, as condições da Dispensa de Licitação nº _____, seus anexos, e de conformidade com a própria proposta comercial da CONTRATADA, conforme descrito abaixo:

ITEM	DESCRIÇÃO	PERIODO	QTD	TIPO	VALOR UNIT. R$	VALOR TOTAL R$
1.	**Licenciamento e Serviços**					
1.1.	**Renovação** da solução de antivírus ESET PROTECT Advanced.	36 meses	75	Licenciamento		
1.2.	**Serviço** de suporte técnico, atendimento 8x5 (oito horas por dia, cinco dias por semana), console de gerenciamento em	36 meses	01	Serviço		

	nuvem e monitoramento 24x7 (tempo integral)					
VALOR TOTAL DA PROPOSTA R$						
POR EXTENSO:						

CLÁUSULA TERCEIRA - DO FUNDAMENTO LEGAL

3.1. O presente contrato decorre do Processo Administrativo nº __/2025, Dispensa de Licitação nº __/2025, regido pelo disposto na Lei nº 14.133/2021, com as alterações posteriores, Lei Complementar nº 123/2006 e demais normas pertinentes ao objeto.

CLÁUSULA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes da execução do presente contrato correrão à conta do recurso orçamentário: 3.3.90.40 – Serviços de Tecnologia da Informação e Comunicação.

CLÁUSULA QUINTA - DO VALOR DO CONTRATO E DA FORMA DE PAGAMENTO

5.1. 1 O valor total do presente contrato é de R$ ... (...).

5.2. O pagamento será realizado no prazo máximo de até 5 (cinco) dias, contados a partir do recebimento da Nota Fiscal/Fatura devidamente atestada pela competente área, por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pela Contratada, ou através de boleto bancário com vencimento mínimo de 5 (cinco) dias.

5.3. Constatando-se alguma irregularidade da Contratada, será providenciada sua notificação, por escrito, para que, no prazo de 05 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Administração Contratante.

5.4. Não será iniciada a contagem de prazo caso os documentos fiscais apresentados ou outros necessários contenham incorreções.

5.5. Quando for constatada qualquer irregularidade na nota fiscal, a CONTRATANTE solicitará imediatamente a CONTRATADA carta de correção, quando couber, ou ainda a pertinente regularização, que deverá ser encaminhada à Contabilidade da Câmara Municipal de Carapicuíba, no prazo de 3 (três) dias úteis.

5.6. Caso a CONTRATADA não apresente carta de correção no prazo estipulado, o prazo para pagamento será reiniciado a partir da data da sua apresentação.

5.7. Todo e qualquer pagamento será efetuado direta e exclusivamente à CONTRATADA, eximindo-se a CONTRATANTE de obrigações a terceiros por títulos colocados em cobrança, descontos, caução ou outra modalidade de circulação ou garantia, inclusive quanto a direitos emergentes desta, ficando estabelecido

que, em hipótese alguma, aceitará tais títulos, os quais serão devolvidos, incontinente, à pessoa física ou jurídica que os houver apresentado.

5.8. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação qualquer obrigação financeira de penalidade que lhe tenha sido imposta.

5.9. A Câmara Municipal de Carapicuíba não se responsabilizará por quaisquer autuações fiscais e gravames futuros decorrentes de interpretações errôneas por parte do licitante vencedor quanto à aplicação de tributos e suas alíquotas, suspensões, base de cálculo, isenções etc.

CLÁUSULA SEXTA – DO REAJUSTE DE PREÇOS

6.1. O valor do contrato poderá ser alterado ou atualizado em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos produtos, nas seguintes situações:

6.1.1. Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuada, nos termos da alínea "d" do inciso II do caput do art. 124 da Lei nº 14.133/2021;

6.1.2. Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre o valor do contrato;

CLÁUSULA SÉTIMA - DA VIGÊNCIA

7.1. O prazo de vigência do Contrato será de 36 (trinta e seis) meses contados da data de sua assinatura, findo o qual será automaticamente reincidido.

CLÁUSULA OITAVA – FORMA DE EXECUÇÃO DO CONTRATO

8.1. Do prazo, do local e das condições de prestação dos serviços

8.1.1 O prazo para entrega do objeto será de até 10 (dez) dias úteis, contados do recebimento do Pedido de Compra.

8.1.2. O pedido será emitido pelo Setor de Compras.

8.1.3. Os serviços serão prestados na Sede da Câmara Municipal de Carapicuíba/SP, localizada na Travessa Virginio Pasini, 63 – Jardim São Pedro, Carapicuíba – SP , CEP: 06320-000.

8.1.4. As despesas de custeio com deslocamento, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos, ficam a cargo exclusivo da Contratada;

CLÁUSULA NONA – DO RECEBIMENTO

9.1. Os serviços serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e

fiscalização do contrato, para efeito de verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

9.2. Os serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 dias úteis, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

9.3. O recebimento definitivo ocorrerá no prazo de 5 dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

9.4. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

9.5. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

9.6. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

9.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens nem a responsabilidade ético-profissional pela perfeita execução do contrato.

CLÁUSULA DÉCIMA – OBRIGAÇÕES DO CONTRATANTE

10.2.1. Receber, acompanhar, fiscalizar, conferir e avaliar o objeto do contrato afim de que sejam executados rigorosamente em conformidade com o estabelecido no processo de contratação;

10.2.2. A fiscalização do contrato, por parte do Contratante, não exonera nem diminui a completa responsabilidade da Contratada por inobservância ou omissão a qualquer das cláusulas contratuais estabelecidas no ajuste;

10.2.3. Notificar a Contratada de qualquer irregularidade constatada, por escrito para que seja sanada;

10.2.4. Efetuar o pagamento nas condições e nos preços pactuados em contrato.

10.2.5. Aplicar à contratada as penalidades regulamentares e contratuais.

CLÁUSULA DÉCIMA PRIMEIRA - OBRIGAÇÕES DA CONTRATADA

11.3.1. Fornecer o objeto em estrita conformidade com as especificações e condições estabelecidas no Processo Administrativo nº ___/2025, Dispensa de Licitação nº __/2025, termo de referência, proposta apresentada e demais condições estabelecidas em contrato;

11.3.2. Manter-se em compatibilidade com as obrigações assumidas no contrato durante toda a sua execução, conservando todas as condições de habilitação e qualificação exigidas na contratação;

11.3.3. Designar preposto para representar a Contratada na execução do contrato.

11.3.4. Prestar todos os esclarecimentos que forem solicitados pela Câmara Municipal, obrigando-se a atender, de imediato, todas as reclamações a respeito dos serviços prestados.

11.3.5. Responsabilizar-se por quaisquer prejuízos que causar à Contratante em decorrência do não cumprimento ou cumprimento irregular das obrigações assumidas;

11.3.6. Arcar com o pagamento de quaisquer tributos, multas ou ônus oriundos da contratação, pelos quais seja responsável, principalmente os de natureza fiscal e comercial;

11.3.7. Atender prontamente às notificações, reclamações, exigências ou observações feitas pela Contratante, refazendo ou corrigindo, quando for o caso, às suas expensas, o objeto que eventualmente tenha sido executado em desacordo com o combinado;

11.3.8. Não transferir, no todo ou em parte, o presente contrato;

11.3.9. Cumprir outras obrigações previstas no Código de Proteção e Defesa do Consumidor (Lei Federal nº 8.078, de 11 de setembro de 1990) que sejam compatíveis com o regime de direito público.

CLÁUSULA DÉCIMA SEGUNDA - GARANTIA DE EXECUÇÃO

12.1 Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA TERCEIRA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

13.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, a CONTRATADA que:

13.1.1. Der causa à inexecução parcial do contrato;

13.1.2. Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

13.1.3. Der causa à inexecução total do contrato;

13.1.4. Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

13.1.5. Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

13.1.6. Praticar ato fraudulento na execução do contrato;

13.1.7. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

13.1.8. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

13.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

13.2.1. Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

13.2.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nos subitens 13.1.2, 13.1.3. e 13.1.4 deste contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

11.2.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nos subintes 13.1.5, 13.1.6, 13.1.7 e 13.1.8 deste contrato, bem como nos subitens 13.1.2, 13.1.3 e 13.1.4, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

13.2.4 Multa moratória de 0,5% (cinco décimos por cento) por dia de atraso injustificado na execução do objeto contratado, sobre o valor da parcela executada em desconformidade com o prazo previsto no contrato ou instrumento equivalente, até o limite de 30 (trinta) dias, nos termos do §3º do art. 156 da Lei n. 14.133/2021. O atraso superior a 30 (trinta) dias autorizará a Administração a promover o cancelamento do contrato, por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei nº 14.133, de 2021;

13.2.4.1. O valor máximo da multa será equivalente a 30 (trinta) dias corridos de atraso. A partir deste momento, além da multa, aplica-se o impedimento de licitar e contratar do item

13.2.2, podendo, à critério da Administração, configurar inexecução total da obrigação assumida, culminando na rescisão do contrato.

13.2.5. Multa compensatória de 20% (vinte por cento) sobre o valor da parcela não cumprida, no caso de inexecução parcial, observado que o valor final apurado para a multa não poderá ser inferior a 0,5% (cinco décimos por cento) do valor total do contrato, nos termos do § 3º do art. 156 da Lei n. 14.133/2021;

13.2.6. Multa compensatória de 30% (trinta por cento) sobre o valor anual do contrato, no caso de inexecução total.

13.3. A aplicação das sanções previstas neste contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao CONTRATANTE (art. 156, §9º, da Lei nº 14.133, de 2021).

13.4. Todas as sanções previstas neste contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

13.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021);

13.4.2 Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo CONTRATANTE a CONTRATADA, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021);

13.4.3. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

13.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa a CONTRATADA, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

13.6. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

13.6.1. A natureza e a gravidade da infração cometida;

13.6.2. As peculiaridades do caso concreto;

13.6.3. As circunstâncias agravantes ou atenuantes;

13.6.4. Os danos que dela provierem para a Administração Pública;

13.6.5. A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

13.7. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

13.8. A personalidade jurídica da CONTRATADA poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a CONTRATADA, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021);

13.9. O CONTRATANTE deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de

publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal (art. 161, da Lei nº 14.133, de 2021).

13.10. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

CLÁUSULA DÉCIMA QUARTA – DA FISCALIZAÇÃO E GESTÃO DO CONTRATO

14.1. Os gestores e fiscais de contratos e os respectivos substitutos serão representantes da Câmara Municipal de Carapicuíba/SP designados pela autoridade competente, com atribuições de acompanhar e fiscalizar a execução do contrato, nos termos dos art. 21 a 23, observados os requisitos estabelecidos no art. 11, do Ato da Mesa nº 7/2024, de 11 de dezembro de 2023, que regulamenta a Lei nº 14.133, de 1º de abril de 2021, no âmbito da Câmara Municipal de Carapicuíba.

14.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade ou ainda resultante de imperfeições técnicas, vícios redibitórios, não implica em corresponsabilidade do Contratante ou de seus agentes e prepostos.

CLÁUSULA DÉCIMA QUINTA – DA SUBCONTRATAÇÃO

15.1. É vedado à CONTRATADA subcontratar, ceder ou transferir, no todo ou em parte, o objeto do presente contrato.

CLÁUSULA DÉCIMA SEXTA – DAS ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

16.2 O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do termo de contrato.

16.4. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos ou previsão normativa, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei no 14.133, de 2021).

16.5 Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA SÉTIMA – DA EXTINÇÃO DO CONTRATO

17.1. O presente Termo de Contrato poderá ser extinto nas hipóteses previstas no art. 137 e 138, da Lei nº 14.133/2021 ou art. 69, inc. VII, da Lei nº 13.303/2016, sem prejuízo da aplicação das sanções previstas neste instrumento.

17.2. Os casos de extinção contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à ampla defesa e ao contraditório.

17.3. A ocorrência de fatos fortuitos ou de força maior, regularmente comprovados, que impeçam a execução do presente contrato.

CLÁUSULA DÉCIMA OITAVA – DOS CASOS OMISSOS

18.1. Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos, além do contido na legislação municipal.

CLÁUSULA DÉCIMA NONA – DA PUBLICAÇÃO

19.1. A CONTRATANTE providenciará as publicações exigidas no art. 72, parágrafo único, e no art. 94, II c/c o art. 176, parágrafo único, inc. I da Lei nº 14.133/21.

CLÁUSULA VIGÉSIMA – DO FORO

20.1. Fica eleito o foro da Comarca de Carapicuíba, Estado de São Paulo, como único competente para conhecer e dirimir quaisquer questões oriundas do presente contrato, com expressa renúncia a qualquer outro, por mais privilegiado que seja.

E, por estarem às partes justas e contratadas, assinam o presente termo em 3 (três) vias de igual teor, na presença das testemunhas abaixo identificadas.

Carapicuíba, ...

CONTRATANTE
CONTRATANTA
TESTEMUNHAS

CONTRATOS OU ATOS JURÍDICOS ANÁLOGOS
TERMO DE CIÊNCIA E DE NOTIFICAÇÃO
Contratos

CONTRATANTE: CÂMARA MUNICIPAL DE CARAPICUÍBA

CONTRATADO:

CONTRATO Nº: __/2025

OBJETO: 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.

ADVOGADO(S)/ Nº OAB: Ana Paula Dias Nicácio / Nº. OAB 192392.

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

a) o ajuste acima referido estará sujeito a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;

b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, conforme dados abaixo indicados, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;

c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;

d) Qualquer alteração de endereço – residencial ou eletrônico – ou telefones de contato deverá ser comunicada pelo interessado, peticionando no processo.

2. Damo-nos por NOTIFICADOS para:

a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;

b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

LOCAL e DATA: Carapicuíba, ...

GESTOR DO ÓRGÃO/ENTIDADE:
Nome:
Cargo:
CPF: RG:
Data de Nascimento:
Endereço residencial completo:
E-mail Institucional:
E-mail pessoal:
Telefone:
Assinatura:_____

Responsáveis que assinaram o ajuste:

Pelo CONTRATANTE:
Nome: Ronaldo de Souza
Cargo: Presidente
CPF: [redacted] RG: [redacted]
Data de Nascimento: [redacted]
Endereço residencial completo: [redacted]
E-mail institucional: [redacted]
E-mail pessoal: [redacted]
Telefone(s): [redacted]
Assinatura:_____

Pela CONTRATADA:
Nome:
Cargo:
CPF: RG:
Endereço residencial completo:
E-mail institucional:
E-mail pessoal:
Telefone(s):
Assinatura: _____