Termo de Referência

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS OBRIGATÓRIAS

O presente Anexo tem como objetivo apresentar as especificações técnicas mínimas dos itens em licitação pela Prefeitura Municipal de Lençóis Paulista, para renovação de sua infraestrutura da Tecnologia da Informação. Os itens especificados em termos de suas principais características, componentes e subcomponentes que os integram e garantem seu perfeito funcionamento, com níveis de desempenho adequados aos fins a que se destinam no contexto de modernização da Administração Pública Municipal.

Quaisquer referências aos itens licitados, nos demais documentos que compõe o processo licitatório, inclusive naqueles apresentados pelos licitantes, deverão estar de acordo com as denominações apresentadas neste Termo, inclusive quanto a sua enumeração.

LICENÇA DE USO ESET PROTECT ADVANCED CLOUD

➔Tipo:

1. Aquisição de licença de uso de software Antivírus, ESET Protect Advanced Cloud, com manutenção até julho de 2025 e suporte 24x7.
2. Renovação de licença de uso de software Antivírus, ESET Protect Advanced Cloud, com manutenção até julho de 2025 e suporte 24x7.

➔Quantidades de licenças:

	Quantidade	Licença
Aquisição	301	ESET Protect Advanced Cloud
Renovação	210	ESET Protect Advanced Cloud

➔Especificações:

Apresentar atestado de capacitação técnica, emitida por empresa de direito público ou privado, no fornecimento das licenças.

Será exigido um prazo mínimo até julho de 2025, para garantia de funcionamento da solução.

Durante o prazo de garantia até julho 2025 deverão ser fornecidas gratuitamente todas as atualizações disponíveis incluindo novas versões da aplicação e das bases de dados de malwares, spywares, etc..

Após o prazo de garantia, a solução deve continuar em funcionamento sem depender de licenças adicionais (excetuando-se licenças de novas versões da aplicação e das bases de dados de malwares, pywares, etc.).

Deverá estar incluso a prestação de suporte técnico via telefone à solução durante o período ate julho de 2025 pelo próprio fabricante da solução.

O suporte deverá ser realizado em pelo menos 30 minutos para início de atendimento em chamados de severidade 1.

Regime de 24x7x365 para o suporte técnico com atendimento por telefone.

Regime de 24x7x365 para acesso as mais recentes atualizações e patches.

Tanto a aquisição quanto a renovação das licenças devem ser incluídas no contrato existente EAV-0358874319 já presente na ESET Business Ac-

count, tendo o mesmo vencimento em 29/07/2025, que hoje consta com 281 licenças e totalizará com 788 licenças.

ESPECIFICAÇÕES

1) ESPECIFICAÇÕES TÉCNICAS:

1.1) Console de gerenciamento centralizada:

1.1.1) O software deve dispor de gerenciamento com administração centralizada na nuvem, com facilidades para instalação, administração, monitoramento, atualização e configuração, com todos os módulos de um único fornecedor.

1.1.2) O acesso ao Console de Gerenciamento deve ser possível via tecnologia Web segura (HTTPS) compatível, no mínimo, com os navegadores Google Chrome, Mozilla Firefox, Microsoft Edge, Opera e Safari.

1.1.3) O acesso ao Console deve suportar várias sessões simultâneas.

1.1.4) Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas.

1.1.5) Mecanismo de comunicação randômico (pull) entre o cliente e o servidor, para consulta de novas configurações e assinaturas, evitando sobrecarga de rede e/ou no servidor.

1.1.6) Permitir o agrupamento dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio.

1.1.7) O servidor de gerenciamento deve possuir compatibilidade para instalação nos seguintes sistemas operacionais em todas as versões/distribuições/releases e Hypervisors:

a) Microsoft Windows 8 / 8.1 Pro.
b) Microsoft Windows 10.
c) Microsoft Windows Server 2012 R2.
d) Microsoft Windows Server 2016.
e) Microsoft Windows Server 2019.
f) Ubuntu 16.04.1 LTS x86 Desktop.
g) Ubuntu 16.04.1 LTS x86 Server.
h) Ubuntu 16.04.1 LTS x64 Desktop.
i) Ubuntu 18.04.1 LTS x64 Desktop.
j) Ubuntu 18.04.1 LTS x64 Server.
k) Ubuntu 20.04 LTS x64.
l) RHEL Server 7 x64.

m) RHEL Server 8 x64.
n) CentOS 7 x64.
o) CentOS 8 x64.
p) SLED 15 x64.
q) SLES 11 x64.
r) SLES 12 x64.
s) SLES 15 x64.
t) OpenSUSE Leap 15.2 x64.
u) Debian 9 x64.
v) Debian 10 x64.
w) Fedora 31 x64.
x) Fedora 32 x64.
y) VMware vSphere/ESXi 6.5 e posterior.
z) VMware Workstation 9 e posterior.
aa) VMware Player 7 e posterior.
ab) Microsoft Hyper-V Server 2012, 2012 R2, 2016, 2019.
ac) Oracle VirtualBox 6.0 e posterior.
ad) Citrix 7.0 e posterior.

1.1.8) O servidor de gerenciamento deve possuir compatibilidade para instalação em sistemas operacional de 64-bits tanto em ambiente virtual quanto físico, disponibilizado pela CONTRATANTE.

1.1.9) Possuir integração com LDAP e Active Directory, para importação da estrutura organizacional e autenticação dos Administradores.

1.1.10) Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede.

1.1.11) Possibilidade de criar grupos separando as regras aplicadas a cada dispositivo.

1.1.12) Possibilidade de instalação dos clientes em estações de trabalho e servidores podendo estes ser físicos ou virtualizados, via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso).

1.1.13) Possibilitar a remoção, de forma automatizada das soluções dos principais fabricantes atualmente instalados nas estações de trabalho e ou servidores da CONTRATANTE.

1.1.14) Descobrir automaticamente as estações da rede que não possuem o cliente instalado através de funcionalidade integrada ao console de gerenciamento.

1.1.15) Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota.

1.1.16) A console de gerenciamento deve apresentar funcionalidade que impeça o usuário de alterar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente.

1.1.17) Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação (minimamente os níveis de operador e administrador).

1.1.18) O log deve ser centralizado e conter, no mínimo, os seguintes itens:

a) Nome da ameaça.
b) Nome do arquivo infectado.
c) Data e hora da infecção.
d) Ação tomada.
e) Endereço de IP da máquina.
f) Usuário autenticado na máquina.
g) Origem da ameaça (IP ou hostname da máquina) caso a ameaça tenha se propagado.

1.1.19) O console de gerenciamento deve prover alertas de segurança via e-mail, com informações de infecção de máquinas e ataques.

1.1.20) Utilizar o protocolo HTTPS ou outro protocolo seguro para comunicação entre console de gerenciamento e o cliente gerenciado.

1.1.21) Capacidade de voltar (rollback) para versão de atualização (da solução ou vacina) através de procedimento específico no console de gerenciamento.

1.1.22) Interface da Console de Gerenciamento totalmente em português.

1.1.23) Possuir manuais em português e inglês.

1.1.24) O fabricante deverá ter documentação publicada na internet no idioma português.

1.1.25) Deve permitir criar o backup da Base de dados da Console de gerenciamento.

1.1.26) O acesso a console de gerenciamento deverá ser autenticado.

1.1.27) A console deverá funcionar também através de um Appliance Virtual fornecido pelo fabricante.

1.1.28) O console de administração de licenças deve ser na nuvem, aonde é possível revisar os detalhes dos equipamentos que estão utilizando a licença do antivírus.

1.1.29) O acesso ao console de administração do antivírus deve permitir a possibilidade de ser feito com duplo fator de autenticação integrado dentro da mesma console aonde é possível ativá-lo sem a necessidade de nenhum add-on adicional.

1.1.30) Gerar pacotes de instalação dos clientes, para cada tipo de sistema operacional existente na estrutura da CONTRATANTE, possibilitando a gravação em mídia e a instalação do software em ambientes onde não seja possível a instalação via rede corporativa.

1.1.31) Permitir forçar a instalação do software cliente do antivírus nos computadores, reinstalando-o em caso de desinstalação ou corrupção do mesmo.

1.1.32) Atualização de vacinas sem a necessidade de reinicialização.

1.1.33) Suportar o gerenciamento de todos os clientes instalados nas máquinas (estações de trabalho, servidores, tablets e smartphones) a partir do servidor de Console de Gerenciamento, oferecendo a possibilidade de configuração centralizada e remota de todas as funcionalidades.

1.1.34) Gerenciar de forma remota as configurações do firewall local de cada máquina com o cliente instalado.

1.1.35) Criação de grupos e subgrupos de máquinas baseada na hierarquia do Active Directory e LDAP ou em identificador único de clientes, tal como endereço IP.

1.1.36) Forçar a configuração determinada no servidor para os clientes, protegendo o software cliente de alterações pelos usuários, com senha pré-determinada na console de gerenciamento.

1.1.37) Atualização/sincronização de configurações nos clientes sem a necessidade de reinicialização ou logoff.

1.1.38) Permitir a criação de tarefas de rastreamento em períodos de tempo pré-determinados e na inicialização do sistema operacional.

1.1.39) Permitir a criação de tarefas de atualização de vacinas e novas versões de software em períodos de tempo pré-determinados.

1.1.40) Permitir criação das tarefas para uma máquina, um grupo de máquinas e/ou para todas as máquinas.

1.1.41) Possuir no mínimo 42 modelos de relatórios pré configurados com filtros e conjuntos de filtros na console de gerenciamento.

1.1.42) Geração de relatórios, permitindo a customização dos mesmos e a exportação para os seguintes formatos (no mínimo um deles):

a) HTML.
b) CSV ou TXT.
c) PDF.

1.1.43) Geração de relatórios que contenham as seguintes informações:

a) Máquinas com a lista de definições de vírus desatualizada, ou todas as máquinas e suas respectivas versões da lista de definições de vírus.
b) Versão do software instalado em cada máquina.
c) Vírus que mais foram detectados. d) Máquinas que mais sofreram infecções em um determinado período de tempo.

1.1.44) Permitir o armazenamento em um banco de dados centralizado das informações coletadas nos clientes:

a) Registro de eventos (log).
b) Relatórios de eventos de vírus e status dos clientes.
c) Relatórios de Softwares instalados.
d) Relatórios de Hardware encontrados.

1.1.45) Fornecer, em tempo real, o status atualizado das estações de trabalho.

1.1.46) Possibilitar a exportação, em formato PDF e CSV, de relatórios que atuem com inventário de hardware e software de todas as estações e servidores ativos na estrutura da console de gerenciamento.

1.1.47) Possuir mecanismo de detecção baseado em ferramentas de análise e detecção como:

a) Machine Learning.
b) Instrusion Prevention System.
c) Inteligência Artificial.

1.1.48) Possuir módulo de proteção em tempo real do sistema de arquivos, o qual deve controlar todos os arquivos no sistema a fim de detectar código malicioso quando os arquivos são abertos, criados ou executados.

1.1.49) Possuir módulo de detecção proativa que forneça proteção contra uma nova ameaça durante a propagação inicial.
1.1.50) Empregar proteção baseada em nuvem conectada diretamente aos laboratórios de pesquisa e desenvolvimento do fabricante.
1.1.51) Possuir módulo nativo de detecção e proteção contra variantes de ransomware existentes no mundo, a fim de atuar como um escudo contra este tipo de ameaça.
1.1.52) Permitir a instalação remota do agente e produto de segurança através de GPO ou SCCM.
1.1.53) Por meio do console de gerenciamento em nuvem deve ser possível gerenciar dispositivos móveis iOS e Android e ter um banco de dados separado do restante dos servidores e estações de trabalho.
1.1.54) O módulo de gerenciamento de dispositivos móveis deverá possuir arquitetura padrão de soluções MDM (Mobile Device Management) do mercado.
1.1.55) O gerenciamento em dispositivos IOS deverá requerer certificado do serviço de notificação por push da Apple, a fim de possibilitar uma comunicação segura entre o servidor e o device.
1.1.56) A solução deve ser capaz de fazer a varredura em um estado ocioso para fornecer proteção proativa enquanto o equipamento não está em uso.
1.1.57) A solução deve possuir um cache local para aumentar o desempenho dos ambientes virtuais, garantindo que o arquivo seja verificado apenas uma vez.
1.1.58) Através da console de gerenciamento a solução deve possibilitar a ativação da opção de bloqueio de exploit por meio do módulo de firewall nas estações e servidores.
1.1.59) Atualização incremental e on-line das vacinas.
1.1.60) A solução deve possuir Sandbox na nuvem para analisar o comportamento de malwares, com SLA de 5 minutos até 1 hora de resposta.
1.1.61) Deve ter a capacidade de utilizar o módulo Sandbox na nuvem para bloquear ameaças de rede a fim de impedir que sejam executadas nas estações de trabalho.
1.1.62) O Sandbox na nuvem deve ser capaz de identificar e bloquear ameaças de dia zero.

1.1.63) A funcionalidade de Sandbox na nuvem deverá ser gerenciada na mesma console principal, permitindo o envio de arquivos para análise de maneira integrada.
1.1.64) A funcionalidade de Sandbox na nuvem deverá possibilitar que o usuário decida como tratar o arquivo analisado.
1.1.65) A tecnologia de Sandbox deve ser baseada em ferramentas de desenvolvimento como: inteligência artificial e machine learning.
1.1.66) Atualização em clientes móveis (notebook, laptop, netbook, ultrabook, e similares) a partir do site do fabricante do antimalware ou de outra fonte definida pelo administrador.
1.1.67) Capacidade de configurar políticas móveis para quando um computador estiver fora da estrutura de proteção, possa atualizar-se via internet.
1.1.68) Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento e Site do Fabricante.
1.1.69) Possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função.
1.1.70) Nas atualizações das configurações e das definições de malwares não se poderá fazer uso de logon scripts, agendamentos ou tarefas manuais ou módulos adicionais que não sejam parte integrante da solução.
1.1.71) Qualquer atualização deve ser possível sem a necessidade de reinicialização do computador ou serviço para aplicá-la.
1.1.72) Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária.
1.1.73) O sistema deve fornecer um único e mesmo arquivo de vacina de malwares para todas as versões do Windows e do antimalware, sendo aceitável arquivos diferentes, para plataformas 32-bits e 64-bits.
1.1.74) Possuir módulo de criptografia de disco gerenciado pela console central para estações de trabalho Windows.
1.1.75) Possibilitar a opção de criptografar apenas o disco de inicialização.
1.1.76) Possibilitar que as estações de trabalho sejam criptografas sem que o recurso de TPM (Trusted Platform Module) esteja válido.

1.1.77) Através da console deve ser possível ativar a criptografia de disco nas máquinas clientes.
1.1.78) Através da console deve ser possível instalar a criptografia de disco nas máquinas clientes.
1.1.79) Através da console central deve ser possível invalidar a senha de login do usuário e solicitar que mude sua senha de login por meio de uma interface gráfica.
1.1.80) Deve possibilitar que o administrador recupere os dados caso o usuário não consiga acessar a máquina com suas credenciais.
1.1.81) Deve possibilitar que o administrador gere uma nova senha de recuperação para o usuário.

1.2) Solução de Antivírus para as estações e servidores:
1.2.1) A solução ofertada deve suportar sistemas operacionais com arquitetura 32-bits e 64-bits.
1.2.2) Gerenciado através de Console de Gerenciamento.
1.2.3) Interface do software cliente em português.
1.2.4) Manuais em português.
1.2.5) O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade para instalação com os seguintes sistemas operacionais em todas as versões/distribuições/releases:
a) Microsoft Windows 7.
b) Microsoft Windows 8. c)
c) Microsoft Windows 8.1.
d) Microsoft Windows 10.
e) Microsoft Windows 2008 server.
f) Microsoft Windows 2008 R2 server.
g) Microsoft Windows 2012 R2 server e/ou superior.
h) Red Hat.
i) SUSE.
j) Ubuntu.
k) CentOs.
l) Debian.
m) Fedora.
n) MacOS 10.12 Sierra.
o) MacOS 10.13 High Sierra.

p) MacOS 10.14 Mojave.
q) MacOS 10.15 Catalina.
r) Android 5 e versões posteriores.
s) IOS 9 e versões posteriores.

1.2.6) O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede.

1.2.7) Possuir módulo de gerenciamento de dispositivos móveis Android e iOS.

1.2.8) Possibilitar a instalação da solução de segurança aos dispositivos móveis de maneira manual através de QRcode, link gerado pela solução de gerenciamento e e-mail.

1.2.9) O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento.

1.2.10) Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes através de comunicação com uma nuvem de dados fornecida pelo fabricante.

1.2.11) Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento.

1.2.12) Permitir o rastreamento de malware, agendado ou manual, com a possibilidade de selecionar como alvo uma máquina ou grupo de máquinas, com periodicidade mínima diária.

1.2.13) O cliente gerenciado deve implementar funcionalidade em que as configurações, alteração, desinstalação, desativação do serviço, importação e exportação de configurações possam ser bloqueadas por senha, através do console de modo a evitar que o usuário da estação de trabalho interfira no funcionamento da solução.

1.2.14) Atualização de configurações, sem interação (em background), nos clientes sem a necessidade de reinicialização ou logoff.

1.2.15) Capacidade de tratar ameaças que exploram a ausência de correções do Sistema Operacional (PATCHES) fazendo com que as ameaças que se utilizam de vulnerabilidades sejam bloqueadas enquanto a correção oficial não esteja instalado/disponível corretamente, ou possuir análise heurística ou inteligência artificial (machine learning) capaz de

identificar e bloquear qualquer ameaça externa que se utilize de vulnerabilidades dos sistemas operacionais.

1.2.16) Caso a solução encontre algum arquivo mal-intencionado (tais como ameaça dia-zero, ameaça persistente), deve possuir capacidade de análise e posterior bloqueio automático.

1.2.17) A função de Escaneamento de vírus deverá ter a possibilidade de configuração de exceções:

a) Excluir da verificação tipos de arquivos tais como .TXT (arquivo de texto simples).

b) Pastas e arquivos pré determinados através do caminho ou Hash.

1.2.18) Deve permitir a instalação e desinstalação remota pela console de gerenciamento centralizada.

1.2.19) Possibilidade de instalação presencial através de mídia de instalação fornecida ou gerada através do servidor de antivírus.

1.2.20) Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, com frequência (no mínimo diária) e horários definidos na console de gerenciamento centralizada:

a) Permitir atualização incremental da lista de definições de vírus.

b) Permitir atualização por endereço do próprio fabricante, como opção além do servidor local.

c) Permitir configuração remota de ordem de preferência de endereços de atualização.

d) Permitir configurar conexão através de serviço Proxy local.

e) Permitir a atualização da lista de arquivos a serem verificados contra vírus através da lista de definições de vírus.

1.2.21) No sistema operacional Linux além de proteger e rastrear seus sistemas de arquivos, também aos arquivos armazenados em compartilhamentos SAMBA/CIFS ou que de alguma forma estejam disponibilizados para o acesso de clientes Windows em um servidor Linux.

1.2.22) Deve ser capaz de detectar e remover todos os tipos de malwares, incluindo vírus, ransomware, worm, trojan, spyware, rootkit, vírus de macro e códigos maliciosos.

1.2.23) Rastreamento em tempo real para vírus de macro e arquivos criados, copiados, renomeados, movidos ou modificados, inclusive em sessões DOS abertas pelo Windows.

1.2.24) Permitir diferentes configurações de varredura em tempo real, tornando o desempenho do produto mais estável, principalmente em máquinas com baixo desempenho de hardware.

1.2.25) Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo.

1.2.26) Detecção em tempo real e limpeza de programas maliciosos como spywares, ransomware, adwares, jokes, discadores, ferramentas de administração remota e programas quebradores de senha, realizando a remoção desses programas e a restauração de áreas do sistema danificados pelos mesmos, com possibilidade de criar uma lista de exclusão dos programas não desejados, onde a administração seja centralizada pela mesma console de gerenciamento do antivírus.

1.2.27) Rastreamento manual com interface gráfica, customizável, com opção de limpeza.

1.2.28) Rastreamento por linha de comando, parametrizável, com opção de limpeza.

1.2.29) Programação de rastreamentos automáticos do sistema com as seguintes opções:

a) Escopo: todos os drives locais, específicos ou pastas específicas.

b) Ação: somente alertas, limpar automaticamente, apagar automaticamente ou mover automaticamente para área de segurança.

c) Frequência: diária, semanal e mensal.

d) Exclusões: pastas ou arquivos que não devem ser rastreados.

1.2.30) Possuir área de segurança (quarentena) no computador no qual o cliente estiver executando.

1.2.31) Detecção de anomalias através dos métodos de assinatura, heurística e por comportamento.

1.2.32) Proteção contra ameaças via internet. A solução deve conter pelo menos:

a) Ajuste no nível de sensibilidade da detecção.

b) Lista de exceção.

1.2.33) Detecção em tempo real e possibilidade de bloqueio e remoção de malwares provenientes de downloads realizados no ambiente web.

1.2.34) Permitir que a funcionalidade de rastreamento em tempo real na navegação possa ser desabilitada.

1.2.35) Detecção em tempo real e possibilidade de bloqueio e remoção de malwares no conteúdo e anexos de mensagens de correio eletrônico, pelo antivírus cliente, analisando tráfego e suportando principais clientes (no mínimo outlook).

1.2.36) Permitir que a funcionalidade de rastreamento em tempo real de e-mail possa ser desabilitada.

1.2.37) Detecção em tempo real e possibilidade de bloqueio e remoção de malwares nas áreas de armazenamento de dispositivos removíveis, tais como:

a) PenDrive.
b) HD externo.
c) Celulares.
d) Tablets.
e) CD/DVD.
f) Impressora USB.
g) Armazenamento de FireWire.
h) Dispositivo Bluetooth.
i) Leitor de cartão inteligente.
j) Dispositivo de criação de imagem.
k) Modem.
l) Porta LPT/COM.
m) Dispositivo portátil.

1.2.38) O fabricante deve oferecer serviços de segurança da informação como por exemplo: teste de penetração, avaliação de vulnerabilidade ou análise de GAPs.

1.2.39) Detecção, análise e reparação de vírus em arquivos compactados, automaticamente, incluindo pelo menos 05 níveis de compactação, nos formatos mais utilizados no mercado.

1.2.40) Ferramenta de firewall bidirecional local no cliente, com possibilidade de configuração, ativação e desativação através da console de gerenciamento centralizada, contendo filtros especificados por aplicação, protocolo, IP, range de IPs, rede, porta e range de portas.

1.2.41) A ferramenta de firewall local deverá tratar tráfego de entrada e de saída de forma independente.
1.2.42) Deve permitir o bloqueio do "Autorun" nas portas USB ou bloquear automaticamente a execução de qualquer ameaça em dispositivos móveis.
1.2.43) Permitir bloquear a conexão de dispositivos removíveis.
1.2.44) Gerar registro (log) dos eventos de vírus em arquivo.
1.2.45) Gerar relatórios, ao menos, de:
a) Eventos de vírus.
b) Status dos clientes.
c) Status dos Updates.
1.2.46) Gerar notificações de eventos de vírus através de alerta por e-mail, ao menos.
1.2.47) Gerar relatórios incluindo tipos de vírus, nome do vírus e se precisa de atualização do Sistema Operacional.
1.2.48) Fabricante deverá ter suporte local em idioma português.
1.2.49) Fornecer, em tempo real, o status atualizado das estações de trabalho, com pelo menos as seguintes informações:
a) Nome da máquina.
b) Endereço IP da máquina.
c) Malwares não removidos.
d) Status da conexão.
e) Data da vacina.
f) Versão do antivírus instalado.
1.2.50) Possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total.
1.2.51) Permitir a criação de exceções nos escaneamentos de arquivos.
1.2.52) Permitir o bloqueio de dispositivos com base nos seguintes critérios:
a) Fabricante.
b) Modelo.
c) Número de série.
1.2.53) Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URLs acessadas.

1.2.54) O Firewall deve possuir funcionalidade deve suportar os protocolos TCP e UDP.
1.2.55) O Firewall deve reconhecer o tráfego DNS, DHCP e WINS com opção de bloqueio.
1.2.56) Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan e Spoofing e botnet.
1.2.57) Possibilidades de criação de assinaturas personalizadas para detecção.
1.2.58) Possibilidade de agendar a ativação de novas regras do firewall.
1.2.59) Possibilidade de criar regras diferenciadas por aplicações.
1.2.60) Possibilidade de criar regras para bloqueio de todos os executáveis da lista ou liberar somente os executáveis da lista.
1.2.61) Bloqueio de ataques baseado na exploração da vulnerabilidade.
1.2.62) Permitir integração com navegadores WEB para prevenção de ataques.
1.2.63) Realizar proteção usando mecanismo de reputação on-line, reportando informações referentes ameaças durante a navegação web.
1.2.64) Possuir taxa de performance de rede inferior a 70MB (mega bytes) comprovada junto a instituições reconhecidas mundialmente em análises profundas de funcionalidades de fabricantes de soluções de segurança.
1.2.65) O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e engines e possuir analista dedicado a pesquisa de defesas contra ameaças e malwares originados no Brasil. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial.
1.2.66) O fabricante deve possuir um laboratório de análise e detecção de malware na América Latina.
1.2.67) Tenha escritório do fabricante no Brasil.
1.2.68) O fabricante não deve possuir nenhum falso positivo nas provas realizadas pelo VB100 do Virus Bulletin nos últimos dez anos.
1.2.69) O fabricante deve ser citado nos relatórios do MITRE ATT&CK como contribuinte de informações e técnicas de detecção nos últimos anos.
1.2.70) A solução deve prover proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos.

1.2.71) As configurações do antimalware deverão ser realizadas através da mesma console de todos os itens da solução.

1.2.72) Permitir a criação de listas de exceções de arquivos e diretórios (arquivos ou diretórios que não serão varridos em tempo real).

1.2.73) Permitir verificação das ameaças de maneira manual, agendada e em tempo real detectando ameaças no nível do Kernel do sistema operacional fornecendo a possibilidade de detecção de Rootkits.

1.2.74) Possibilitar que, nas varreduras agendadas, o disparo do processo ocorra por grupos com intervalos de tempo determinados, de forma a reduzir impacto em ambientes.

1.2.75) Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar e Ignorar.

1.2.76) Verificação de malwares nas mensagens de correio eletrônico, pelo antimalware da estação de trabalho, suportando clientes Outlook, ou que utilizem os protocolos POP3/SMTP.

1.2.77) Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados.

1.2.78) Deve suportar varredura de, no mínimo, os seguintes padrões de compactação:

a) CAB.
b) ZIP.
c) RAR.
d) LHA.
e) ARJ.
f) TAR.

1.2.79) Capacidade de terminar o processo e serviço da ameaça no momento de detecção.

1.2.80) Capacidade de identificação da origem da infecção, para malwares que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou endereço IP da origem com opção de bloqueio da comunicação via rede.

1.2.81) Possibilidade de bloquear verificação de malware em recursos mapeados da rede.

1.2.82) Capacidade de realizar monitoramento em tempo real por heurística correlacionando com a reputação de arquivos.

1.2.83) Não serão aceitas soluções de Antimalware que possuam engine de terceiros.
1.2.84) Permitir o bloqueio da execução de aplicações baseado em nome e pasta.
1.2.85) A solução deve permitir a detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações.
1.2.86) Capacidade de detecção de keyloggers por comportamento dos processos em memória.
1.2.87) Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo Hosts.
1.2.88) Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção de níveis distintos de sensibilidade de detecção.
1.2.89) Realizar inspeção de ameaças em ambiente isolado, com o emprego de ferramentas como:
    a) Aprendizado de máquina.
    b) Deep Learning.
    c) Análise estatística e dinâmica.
    d) Detecção baseada em comportamento.
    e) Introspecção na memória.
1.2.90) Detecção do malware por DNA do vírus.
1.2.91) O fabricante deve estar presente no Quadrante Mágico do Gartner no último ano, relacionado a plataformas de Endpoint Protection.
1.2.92) Deverá ter a capacidade de atualizar os patches do sistema operacional.
1.2.93) A solução deve ser capaz de detectar o uso do Hyper-V e ter uma verificação de malware específica disponível para este hipervisor.
1.2.94) Em servidores que usam “OneDrive for Business” você deve explorar os arquivos armazenados nesta nuvem, procurando por arquivos comprometidos ou possível malware.
1.2.95) A solução de proteção de servidor deve incluir a detecção e bloqueio de intrusões, adicionando à lista negra os endereços que foram identificados com este comportamento malicioso.
1.2.96) A solução deve adicionar exclusões automaticamente para aplicativos de servidor críticos.

1.2.97) Otimize o desempenho de infraestruturas mistas (hardware e virtual), podendo eliminar a duplicação de verificações de arquivos, excluindo arquivos já verificados e limpos.
1.2.98) Controlar acesso a sites, possibilitando o bloqueio do mesmo.
1.2.99) Permitir criar políticas de bloqueio com base em categorias e lista de URL.
1.2.100) Permitir gerar relatórios de sites acessados e bloqueados.
1.2.101) Permitir a personalização das mensagens exibidas quando um ou mais sites forem bloqueados.
1.2.102) Deverá possuir um plug-in que se integre com o cliente de correio eletrônico como Outlook, Outlook Express e Windows Mail.
1.2.103) Para a navegação na internet o produto deve contar o antiphising para proteger os usuários finais de sites web falsos que tentam obter informações confidenciais.
1.2.104) A solução de proteção Antispam deve realizar as verificações utilizando o protocolo SSL.
1.2.105) Possuir protocolo de replicação que utilize o protocolo HTTPS e o serviço de notificação via push (EPNS).

FORMA DE PAGAMENTO

O pagamento será efetuado da seguinte forma:

a) Pagamento em até 15 (quinze) dias após a entrega das licenças e emissão da nota fiscal.

PREFEITURA MUNICIPAL DE LENÇÓIS PAULISTA
Praça das Palmeiras, 55 – Fone (14) 3269-7000
CEP 18682-900 – Lençóis Paulista – SP
CNPJ: 46.200.846/0001-76
www.lencoispaulista.sp.gov.br

EMISSÃO DAS NOTAS FISCAIS

As Notas Fiscais deverão ser emitidas de acordo com as especificações e indicações para as respectivas secretarias e autarquias:

Prefeitura Municipal de Lençóis Paulista:

Praça das Palmeiras, 55 – Centro – 18682-900
Lençóis Paulista – SP
CNPJ 46.200.846/0001-76

1. Aquisição Licença ESET Protect Advanced Cloud

Quantidade	Licença
137	ESET Protect Advanced Cloud

2. Renovação Licença ESET Protect Advanced Cloud

Quantidade	Licença
84	ESET Protect Advanced Cloud

Secretaria de Educação:

Praça das Palmeiras, 55 – Centro – 18682-900
Lençóis Paulista – SP
CNPJ 46.200.846/0001-76

1. Aquisição Licença ESET Protect Advanced Cloud

Quantidade	Licença
49	ESET Protect Advanced Cloud

2. Renovação Licença ESET Protect Advanced Cloud

Quantidade	Licença
126	ESET Protect Advanced Cloud

Secretaria de Saúde:

Prefeitura Municipal de Lençóis Paulista
Praça das Palmeiras, 55 – Centro – 18682-900
Lençóis Paulista – SP
CNPJ 46.200.846/0001-76

1. Aquisição Licença ESET Protect Advanced Cloud

Quantidade	Licença
105	ESET Protect Advanced Cloud

CMFP – Centro Municipal de Formação Profissional:

Av. Lazaro Brígido Dutra, 101 – Jardim Itamaraty
Lençóis Paulista – SP
CNPJ 51.519.197/0001-00

1. Aquisição Licença ESET Protect Advanced Cloud

Quantidade	Licença
05	ESET Protect Advanced Cloud

SAAE– Serviço Autônomo de Água e Esgotos de Lençóis Paulista:

Rua XV de Novembro, 1.111 – Vila Santa Cecília
Lençóis Paulista – SP
CNPJ 51.426.849/0001-62

1. Aquisição Licença ESET Protect Advanced Cloud

Quantidade	Licença
05	ESET Protect Advanced Cloud

CONDIÇÕES GERAIS

As versões dos softwares ofertados serão as mais novas no mercado, não podendo ser ofertado versão desatualizada ou anterior a comercializada no Brasil pelo fabricante.

Caso haja alteração por motivos de atualizações tecnológicas das versões propostas, a LICITANTE deverá comunicar de imediato no ato da licitação, apresentando a versão substituta, mantendo a administração atualizada e informada sobre o assunto.

No preço total deverá estar incluso todas as despesas que influenciam nos custos, tais como: frete e tributos (impostos, taxas, emolumentos, contribuições fiscais, etc), obrigações sociais, trabalhistas, fiscais, encargos comerciais ou de qualquer natureza, e todos os ônus diretos.

Se houver divergência no Part Number (PN) dos produtos ofertados, a empresa vencedora deverá obrigatoriamente realizar todas as atualizações de acordo com as especificações deste termo de referência e dos registros no fabricante, bem como, deverão ocorrer com os mesmos critérios a inserção das licenças na plataforma de segurança já existente.

A entrega deverá ser realizada integralmente, não sendo aceito entregas parciais.

Lençóis Paulista, 07 de março de 2.023.

Eder Paccola Santa Bárbara
Secretário de Tecnologia da Informação