TERMO DE REFERÊNCIA

1. OBJETO:
O objeto da presente é a aquisição de licenças de uso de software antivírus, para fins de proteção da rede lógica, equipamentos de TI (computadores desktops, notebooks e servidores de dados, etc.) e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, conforme condições, quantidades e exigências estabelecidas neste Termo de Referência.

2. QUANTIDADE E ESPECIFICAÇÃO DO OBJETO:
Aquisição de 50 licenças de uso de software de antivírus, período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses com o objetivo de proteção, rastreamento, localização, bloqueio, quarentena e remoção de ameaças de vírus, trojans, spam, phishing, etc., que possam colocar em risco, invasão e danificar arquivos, dados, computadores, servidores de dados e a rede lógica de computadores corporativa do SAAESP.

2.1 PRINCIPAIS CARACTERÍSTICAS DA SOLUÇÃO DE ANTIVÍRUS:
Antimalware para estações de trabalho;
Antimalware para servidores;
Antimalware para ambientes virtualizados;
Controles de aplicativos;
Controles de dispositivos;
Controles de Endpoint;
Anti-APT - " Advanced Persistent Threat" (ameaça persistente avançada);
A solução deverá possuir Dashboard (console) que forneça visibilidade em tempo real de incidência de malware, status de atualização das máquinas, bem como quaisquer avisos ou erros que possam ocorrer, incluindo;
a) Máquinas com a lista de definições de malware desatualizada;
b) Os malwares que foram detectados;
c) Última comunicação com a console;
d) Data da última varredura (scan) completa;
Gerenciamento unificado e centralizado de todas as funções na mesma console bem como a instalação e atualização dos clientes com a possibilidade de sincronização com o Microsoft Active Directory;
Possibilitar a Instalação Remota dos clientes;
Possuir compatibilidade com protocolo RADIUS para autenticação externa da ferramenta ou ser compatível com o Microsoft Active Directory para os acessos administrativos da ferramenta;

Permitir diferentes níveis de administração da console de gerenciamento utilizando usuários ou grupos do domínio Microsoft Active Directory;

Detecção de comprometimento: vírus, malware, backdoors, hosts em comunicação com sistemas infectados por botnet, serviços da Web vinculados a conteúdo malicioso;
Suporte total aos sistemas operacionais de cliente baseados nas plataformas: Windows 7, 8, 10, 11 ou superior, em todas as suas versões e nas arquiteturas de 32 e 64 bits;
Suporte total aos sistemas operacionais de servidor baseados nas plataformas: Windows 2008 ou superior, inclusive nas arquiteturas de 32 e 64 bits, tanto físicos como virtuais;
Atualizações automáticas das listas de definições de malware a partir de local predefinido da rede, ou de site da Internet;
Frequência de atualização personalizável por dia, semana ou mês;
Varredura em tempo real: de arquivos (gravação, renomeio e leitura), e de processos em memória;
Detecção e remoção de programas maliciosos com spyware, adware, trojans, dialers, rootkits, etc;
Monitoramento em tempo real para a captura de malwares que são executados em memória sem a necessidade de escrever em arquivo;
Capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema através de análise heurística;
Solução única para proteção contra malwares, incluindo vírus, trojans, adware, rootkits, spywares, aplicações potencialmente indesejadas (PUAs), e buffer overflow;
Oferecer proteção avançada de sistemas contra ameaças, tais como ataques aos navegadores;
Possuir proteção contra vulnerabilidades desconhecidas, tais como estouro de buffer (buffer overflow) e ataques de dia zero (zero-day attacks);
Possuir algum método de desinstalação de antivírus corporativos pré-instalados no ambiente;
Possuir instalação "silenciosa" por meio de GPO (Group Policy Object) da Microsoft, scripts de logon, entre outros.
Permitir o gerenciamento do servidor utilizando os protocolos TCP/IP;
Permitir a alteração das configurações dos antivírus nos clientes de maneira remota e/ou por meio de regras aplicáveis a uma máquina, um grupo de máquinas, faixa de IPs;
Permitir a criação de tarefas de atualização, verificação de vírus e upgrades de produto em intervalos de templo pré-definidos;
Permitir o armazenamento das informações coletadas nos clientes em um banco de dados padrão SQL, centralizado ou no próprio servidor da solução;
Permitir enviar a configuração das políticas do servidor para os clientes;
Permitir gerar relatórios, no mínimo, nos formatos: PDF, CSV;
Possuir capacidade de gerar relatórios e gráficos;
O controle de dispositivos deve ocorrer no mínimo para os seguintes dispositivos: a) Dispositivos de armazenamento em massa (ex.: pen drives, memory cards, discos rígidos externos, etc.); b) Drive de CD/DVD/Blue-Ray; c) Modem; d) Dispositivos Wireless;

A solução deverá prover controle de dispositivos com no mínimo as seguintes características: Somente Leitura (Read only), Acesso Completo (Full Access) e

bloqueado (Blocked);
Deve permitir que o administrador defina uma White-List de dispositivos permitidos como Somente Leitura ou Acesso Completo;
Solução de controle de aplicativos para estações e servidores deverá ter, no mínimo, as seguintes características: a) Verificação na execução; b)
Bloqueio da aplicação por seu nome de processo. 3.4.39 Deve permitir bloqueio de navegação em determinados sites com as seguintes características: a)
Lista de categorias específicas conforme o contexto, atualizadas automaticamente pelo fab ricante; b)Opção de adicionar sites em uma lista de liberação de sites que não devem ser bl oqueados (white-list); c)Opção de adicionar sites em uma lista de bloqueio de sites que de vem ser bloqueados (block-list);
Capacidade de verificar a reputação de arquivos;
Deve possuir um controle de modificação do cliente Endpoint e contra a remoção não auto rizada pelo cliente, possuindo uma senha;
Possibilidade de recuperar arquivos da quarentena;
A solução deve possuir cache local na reputação de arquivos, possibilitando não varrer arquivos categorizados como não maliciosos e já "escaneados" anteriormente;
Possibilidade de recuperar instalação em clientes em caso de falha;
Deve ter a capacidade de iniciar à "autoremediação"do computador que falhou a auditoria, ou seja, corrigir os pontos onde a verificação especificada pelo administrador falhou;
Deve ter a possibilidade de notificação customizada para o usuário;
A solução deverá ser capaz de analisar ameaças sem o uso de assinaturas;
A proteção deverá funcionar mesmo que o host esteja off-line;
A solução deverá ter a capacidade de detectar ameaças antes que sejam executadas;
A solução deverá ser capaz de bloquear tanto ameaças conhecidas como também as desconhecidas;
A proteção deverá fazer uso de múltiplas camadas para analisar dados;
Das funcionalidades de proteção contra ransomwares:
Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;
Deve possuir proteger endpoints contra-ataques de ransomware;
Deve automaticamente reverte alterações de arquivos criptografados;
Deve possuir nível forense para identificar e remover malwares;
Para estações de trabalho, dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;
Para servidores, dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;
Deve bloquear técnicas de explorações de vulnerabilidades conhecidas.

3. FORMA, LOCAL E PRAZOS DE ENTREGA DO BEM OU MATERIAL.

A entrega dos itens efetivamente contratados deverá ser entregue preferencialmente no almoxarifado do SAAESP em até 05 (cinco) dias após a expedição da Autorização de

Fornecimento, contando-se o prazo a partir da comunicação formal a empresa vencedora que será efetuada por via e-mail ou outro meio hábil.

O SAAESP poderá rejeitar, no todo ou em parte, o material ou bem adquirido caso esteja em desacordo com as especificações e condições deste Termo de Referência.

4. CONDIÇÕES DE RECEBIMENTO

O recebimento dos bens ou materiais deverá ocorrer de forma provisória, para posterior verificação de conformidade do objeto, e definitivamente, após a verificação das especificações, da qualidade e quantidades dos materiais no prazo máximo de 30 (trinta) dias.

5. JUSTIFICATIVA

- Trata-se de pedido de aquisição de bens e materiais por dispensa de licitação.
- Não há no Almoxarifado do SAAESP o material ou bem a ser adquirido.
- A decisão pela contratação, é o custo/benefício.
- A modalidade de contratação deve ser o menor preço, e os valores ser razoável e mais vantajoso para atender as necessidades da Administração na forma definida neste Termo.
- A opção pela contratação visa atender a Lei Complementar Federal nº 123/2006, o **Decreto Federal nº 8.538/2015 e a** Lei Complementar Municipal nº 70/2011, para as contratações públicas de bens, serviços e obras visando o incentivo e a concessão de tratamento favorecido, diferenciado e simplificado para microempresas e empresas de pequeno porte, agricultor familiar, produtor rural pessoa física, microempreendedor individual - MEI e sociedades cooperativas, com objetivo de promover o desenvolvimento econômico e social no âmbito local e regional, ampliar a eficiência das políticas públicas e incentivar o turismo e a inovação tecnológica, mediante geração de renda, devendo a Administração Pública obedecer aos princípios da eficiência, interesse público, isonomia, legalidade, impessoalidade, moralidade, publicidade.

6. ACOMPANHAMENTO E FISCALIZAÇÃO

O agente público que irá acompanhar e fiscalizar o fornecimento do bem ou material é José Roberto Fantato inscrito no CPF nº 191.621.988.82 e lotado neste setor.

7. CONDIÇÕES DE PAGAMENTO

O pagamento será realizado em até 30 (trinta) dias após a emissão e aceitação da Nota Fiscal pela Secretaria demandante através de depósito ou transferência bancária em conta corrente em nome da empresa sendo admitida conta digital na Nubank.
O documento fiscal deverá, necessariamente estar em nome da empresa fornecedora.

8. OBRIGAÇÕES DA CONTRATADA

O material ou bem deverá estar dentro do prazo de validade.

9. SUPORTE LEGAL
Lei Orgânica do Município de São Pedro
Lei 14.133/2021 (inc. I e II art. 75)
Lei Complementar Federal nº 123, de 14/12/2006
Decreto Federal nº 8.538, de 06/10/2015
Lei Complementar Municipal nº 70, de 30/09/2011
Decreto Municipal nº 7.411, de 19/01/2022

São Pedro, 28 de fevereiro de 2024.

_____
José Roberto Fantato
Departamento de Informática