TERMO DE REFERÊNCIA

1. OBJETO

Contratação de licença de uso de software de anti-virus, pelos período de 12 meses, para o uso da Prefeitura de Itu.

2. JUSTIFICATIVA DA CONTRATAÇÃO

A aquisição das licenças de antivírus tem o objetivo prevenir a contaminação por vírus, malwares e suas variantes bem como ameaças cibernéticas distintas nos computadores da Prefeitura de ITU que podem colocar em risco o sigilo, a integridade e disponibilidade das informações. Com o grande volume de utilização e com o crescimento da utilização de emails e acesso a páginas de internet a aquisição de um software de antivírus é necessária para fornecer um mínimo de segurança à infraestrutura de rede de computadores da Prefeitura de Itu. As aquisições propõem uma maior proteção aos computadores e servidores, resguardando problemas que podem prejudicar os serviços da Prefeitura de Itu. Assim, a aquisição das licenças de antivírus é considerada imprescindível para garantir a disponibilidade, integridade e confiabilidade dos dados e continuidade das atividades da Prefeitura de Itu.

3. DESCRIÇÃO DO OBJETO

3.1. REQUISITOS MÍNIMOS PARA A SOLUÇÃO DE ANTIVÍRUS

3.1.1. Possuir uma única console de gerenciamento para gestão e configurações do antivírus, antispyware, firewall, detecção de intrusão, controle de dispositivos, controle de aplicações e criptografia de discos.

3.1.2. A solução deverá ter a capacidade de remoção do atual antivírus instalado e ser capaz de instalar de forma remota o agente do antivírus pela console de gerenciamento, e caso não tenha a capacidade de realização a remoção completa, a contratada deverá remover a atual solução utilizando scripts, softwares de terceiros, ou mesmo de forma manual;

3.1.3. O produto deverá possuir no mínimo os seguintes módulos e funcionalidades:

3.1.3.1. Console de gerenciamento fornecendo funcionalidades de gestão e configurações de políticas;

3.1.3.2. Módulos para estações físicas, notebooks e servidores;

3.1.3.3. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;

3.1.3.4. Módulo para dispositivos móveis no mínimo para tablets e smartphones com sistema operacional iOS e Android;

3.1.3.5. Utilizar o conceito de heurística para combate e ações contra possíveis malwares;

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

3.1.3.7. Oferecer tecnologia nativa no intuito de eliminar ameaças que sequestram dados, do tipo ransomware;

3.1.3.8. Oferecer inventário de softwares;

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

3.1.3.10. Oferecer proteção por base de assinaturas (vacinas).

3.1.4. Console de Gerenciamento;

3.1.5. Instalação e Configuração:

3.1.5.1. Instalação e configuração

3.1.5.2. Permitir instalação de console local (on-premise) com banco de dados local ou instalação em nuvem (cloud) com banco de dados também em nuvem;

3.1.5.3. Para a opção de console local de ser fornecido como um appliance virtual ou executável para instalação em servidores Windows. Deverá suportar no mínimo as seguintes plataformas de virtualização:

VMWare vSphere;
Citrix XenServer; XenDesktop, VDI-in-a-Box;
Microsoft Hyper-V;
Red hat Enterprise Virtualization;
Kernel-based Virtual Machine ou KVM;
Oracle VM;

3.1.6. Deverá ser fornecido com base de dados embutida e proprietária ou com possibilidade de utilização de banco de dados externo SQL ou Oracle;

3.1.7. Para instalação da console em nuvem (cloud), a nuvem deve ser privada e do mesmo fabricante;

3.1.8. Permitir instalação remota via console WEB de gerenciamento para ambientes virtuais VMWare ou Citrix;

3.1.9. O mecanismo de varredura deverá estar disponível para download separadamente;

3.1.10. A solução deverá permitir a inclusão de um modulo de balanceamento para casos em que vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance, dentre outras necessidades); **3.1.11.** Deve ser totalmente em português.

3.1.12. Licenciamento Flexivel.

3.1.13. A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações:

Nome;
IP;

Sistema Operacional;
Política Aplicada;

3.1.14. A console de gerenciamento deverá incluir sessão de log com as seguintes informações:

Login;
Edição;
Criação;
Log-out;

3.1.15. Arquitetura simples de atualização, com um simples clique deve ser possível atualizar todas funções e serviços da solução;

3.1.16. Permitir que o administrador escolha qual o pacote será atualizado;

3.1.17. As notificações devem ser destacadas como item não lido e notificar o administrador por e-mail;

3.1.18. No mínimo enviar notificações para as seguintes ocorrências:

Problemas com licenças;
Alertas de surto de vírus;
Máquinas desatualizadas;
Eventos de antimalware;
Deverá prover o acesso via HTTPS;
Deverá permitir a importação de certificados digitais;

3.1.19. O gerenciamento e a comunicação com dispositivos móveis deve ser feito de forma segura utilizando certificados digitais.

3.1.20. Monitoramento baseados em "portlets" configuráveis com no mínimo as seguintes especificações:

Nome;
Tipo de relatório;
Alvo do relatório;

3.1.21. Deverá disponibilizar "portlets" para gerência e monitoramento de qualquer tipo de endpoint, máquinas físicas, virtuais e dispositivos móveis.

3.1.22. Inventário da rede;

3.1.23. Possuir no mínimo as integrações abaixo:

Múltiplos domínios do Active Directory;
Múltiplos VMWare vCenters;
Múltiplos Citrix Xen Servers;
Possuir a possibilidade de definição de sincronização com o Active Directory em horas;
Descoberta de rede para máquinas em grupo de trabalho;

3.1.24. Possuir busca em tempo real pelo menos com os seguintes filtros:

Nome;
Sistema Operacional;
Endereço IP;

3.1.25. Possibilitar a instalação remota e desinstalação remota do antivírus;

3.1.26. Possibilitar a configuração de pacotes de instalação do produto de antivírus;
3.1.27. Possuir tarefas remotas e configuráveis de scan
3.1.28. Possuir tarefa de reinicialização remota de estação ou servidor;
3.1.29. Assinar políticas para no mínimo os níveis:
Computador;
Máquina Virtual;
Grupo de Endpoints;
Usuário do AD; Grupo
do AD.
3.1.30. Possuir a propriedade detalhada de objetos gerenciados para:
Nome;
IP;
Sistema Operacional;
Grupo;
Política Assinada;
Ultimo status de malware;
Politicas;
3.1.31. Modelo único para todos os equipamentos, sejam físicos ou virtuais;
3.1.32. Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;
3.1.33. Através da console de gerenciamento o administrador poderá ser capaz de enviar uma política única para configurar o antivírus;
3.1.34. Deverá configurar as funcionalidades como escaneamento do antivírus, firewall de duas vias de detecção de intrusão, controle de acesso a rede, controle de aplicação, controle de acesso web, criptografia (Windows, Mac e Android), localização de dispositivo (Mobile), autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade.
3.1.35. Relatórios:
3.1.35.1. Deverá apresentar as seguintes funcionalidades:
Relatório para cada serviço de segurança;
Facilidade de usar e visualização simplificada;
Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;
Filtros de agendamento de relatórios;
Arquivo com todas as instâncias de relatório agendados;
Exportar o relatório nos formatos .pdf e/ou .csv;
Oferecer possibilidade de criar relatórios de maneira dinâmica no dashboard da da console de gerenciamento;
3.1.36. Administração de usuários.
Deverá apresentas no mínimo as seguintes funcionalidades:
Administração baseada em regras;
Disponibilizar tipos de usuários pré-definidos como no mínimo:

Administrador – Gerente dos componentes da solução;
Administrador de rede - Gerente dos serviços de segurança;
Relatório – Monitora e cria relatórios;

Deverá ser possível customizar um tipo de usuário:

Deverá permitir a integração de usuários com o Active Directory para autenticação da console de gerenciamento;
Registrar as ações do usuário na console de gerenciamento;
Detalhar cada ação do usuário;
Permitir busca complexa baseada em ações do usuário, intervalos de tempo.

3.1.37. Segurança para estações e servidores;

3.1.38. Proteção para ambientes físicos;

3.1.39. Deverá proteger em tempo real e agendado as máquinas físicas em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto na console local (on-premises) como na console em nuvem (cloud);

3.1.40. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho:

Windows 10 64Bits;
Windows 8.1 64Bits;
Windows 8 64Bits;
Windows 7 64Bits;
Windows XP (SP3) apenas o módulo de antivírus;

3.1.41. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores:

Windows Server 2012R2
Windows Server 2012;
Windows Server 2008 R2
Windows Server 2008;
Windows Server 2003 R2 apenas o módulo de antivírus;
Windows Server 2003 com SP1 apenas o módulo de antivírus;

3.1.42. Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux:

Red Hat Enterprise Linux;
Cent OS 5.6 ou superior;
Ubuntu 10.04 LTS ou superior;
SUSE Linux Enterprise Sever 11 ou superior;
OpenSUSE 11 ou superior; Fedora
15 ou superior;
Debian 5.0 ou superior.

3.1.43. Proteção para ambientes virtuais.

Para plataforma de virtualização com VMWare, deverá:

Ter a disponibilidade de ser integrado e oferecer a escaneamento sem instalar o agente nas máquinas virtuais;

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

Deverá proteger em tempo real e agendado as máquinas virtuais em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto na console local (on-premises) como na console em nuvem (cloud);

O produto deverá oferecer agente para virtualização dos seguintes produtos:

Citrix Xen Server;
Microsoft Hyper-V;
VMware ESXi;
Red Hat Virtualization;
Oracle KVM; KVM.

3.1.44. Instalação e Configuração Remota

Deverá permitir ao administrador customizar a instalação;

Deverá permitir a instalação customizada do antivírus com no mínimo: Instalar o antivírus sem o controle de acesso a internet; (Windows Desktop)

Instalar o antivírus sem o módulo de firewall; (Windows Desktop) A instalação deverá ser possível executar com no mínimo das seguintes maneiras:

Executar o pacote de antivírus diretamente na estação de trabalho;

Instalar remotamente, distribuído via console de gerencia web; Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;

Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits;

Deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;

O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário a distribuição em um agente separado.

3.1.45. Funções Gerais:

Deverá ter métodos de detecção de vírus, spyware, rootkits e outros mecanismos de segurança;

Deverá permitir a configuração do scan do antivírus do cliente como:

Scan local;
Scan hibrido (local\remoto);
Scan remoto;

Deverá reportar o estado atual das máquinas virtuais no mínimo, protegida/desprotegida;

Deverá fazer scan em tempo real e automático;

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

Deverá possuir escaneamento baseado em análise heurística; Deverá permitir a escolha e configuração de pastas a serem scaneadas;

Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção:

Baseada em assinaturas;

Baseada em heurística;

Baseada em monitoramento contínuo de processos;

Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL nas estações de trabalho;

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

Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho;

No módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;

3.1.46. Quarentena:

Deverá permitir restauração remota, com configuração de localidade e deleção; Criação e exclusão para arquivos restaurados;

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

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

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

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

Deverá permitir escanear a quarentena após a atualização de assinaturas.

3.1.47. Controle de Usuário

Deverá ter módulo de controle de usuário integrando com as seguintes características:

Bloqueio de acesso a internet;

Bloqueio de acesso a aplicações definidas pelo administrador.

3.1.48. Controle do Dispositivo

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

Através do módulo de controle de dispositivo deverá ser possível controlar:

Bluetooth;

CDROM/DVDROM;

IEEE 1284.4;

IEEE 1394;

Windows Portable;

Adaptadores de Rede;

Adaptadores de rede Wireless;
Discos Externos;

Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como:

CD/DVD;
Discos Externos;
Pen-Drivers;

Deverá permitir regras de definição de bloqueio/desbloqueio; Deverá permitir regras de exclusão.

3.1.49. Criptografia.

Deverá oferecer:

Possibilidade de criptografia de disco através da mesma console de gerenciamento do antivírus, seja em nuvem (cloud) ou local (on-premise);
Deverá utilizar quando necessário serviços de criptografia sem agentes nativos da estação de trabalho seja baseada em Windows ou Mac;
Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;
Deverá ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra.

3.1.50. Atualização

Após a atualização o administrador deverá ter a capacidade de configurar uma reinicialização;
Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
Permitir atualizações de assinatura de hora em hora;
Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.

3.1.51. Segurança para dispositivos móveis

Configurações de Segurança

Caso o dispositivo não esteja em conformidade com as políticas estabelecidas deverá ser possível as ações abaixo:

Ignorar;
Bloquear acesso;
Bloquear o dispositivo;
Restaurar as configurações de fábrica;
Remover o dispositivo da console de gerenciamento;

Deverá permitir o uso de senha. A senha pode ser configurada conforme necessidade do administrador com no mínimo os seguintes recursos:

Senha simples ou complexa;
Números e caracteres;
Comprimento mínimo;
Caracteres especiais mínimos;

Período de expiração da senha;
Definir restrição de reutilização de senha;
Definir o número de tentativas de entradas de senha incorretas; Período de bloqueio do dispositivo.

3.1.52. Segurança de e-mails.

Fornecer proteção de antispam para ambiente com instalação local (onpremise) do MS Exchange;
Oferecer análise comportamental e proteção para zero-day;
Oferecer proteção contra vírus e tentativas de phishing.

4. QUANTIDADES

Segue tabela com as quantidades dos equipamentos:

Item	Descrição do Item	QTD
01	Aquisição de licenças e Atualização de Antivirús, pelo período de 12 meses.	500
02	Suporte técnico pelo período de 12 meses	

5. ENTREGAS

As entregas deverão ser feitas de forma eletrônica, aja vista que são licenças de uso e não possuem material físico.

6. GESTÃO DO CONTRATO

A gestão da prestação de serviço será realizada pela servidora Rafael Henrique de Brito Silva, cargo: Diretor de Informatica, e-mail: rafael.silva@itu.sp.gov.br, telefone: (11) 4886-9877 e a fiscalização será realizada pela CAMILA CAROLINE GONCALVES FERRARI, Cargo: Chefe de GAbinete, E-mail: camila.ferrari@itu.sp.gov.br, Telefone: (11)4886 9802, nas condições de representantes da Prefeitura Municipal de Itu, permitida a contratação de terceiros para assisti-las e subsidiá-las de informações pertinentes a essa atribuição.

7. CONDIÇÕES DE MEDIÇÃO E PAGAMENTO

O prazo de pagamento será de 10 dias fora a quinzena, contados a partir do recebimento do produto.

A contratada receberá o valor previsto, de acordo com sua proposta, dos quais serão deduzidos os descontos previstos na legislação vigente.

8. CRITÉRIO DE SELEÇÃO DO FORNECEDOR

Modalidade escolhida para contratação de fundamento legal Art. 75 inciso 2 da Lei 14133/21.

_____

Rafael Henrique de Brito Silva
Diretor de Informática