ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

O objeto desta licitação compreende a aquisição de solução de antivírus corporativo para estações de trabalho e servidores, treinamento e suporte técnico pelo período de 12 (doze) meses, conforme condições, quantidades e exigências estabelecidas no Anexo I – Termo de Referência.

2. JUSTIFICATIVA

A Prefeitura Municipal de Registro possui um parque de recursos tecnológicos que necessitam de proteção constante. Apesar de facilitadora, a tecnologia da informação inclui novos riscos às informações recebidas, armazenadas ou transmitidas pela Prefeitura Municipal de Registro, o que requer métodos adequados de proteção das informações. Uma das camadas de proteção é realizada pelo sistema de antivírus, atualmente chamado de sistema de proteção de estações de trabalho (Endpoint). Esta camada implementa a segurança das estações de trabalho, servidores e notebooks, oferecendo proteção em tempo real contra as ameaças mais comuns da Internet como vírus, worms e trojans, além de fornecerem opções avançadas de segurança como o bloqueio de dispositivos e análises de ameaças não conhecidas.

DESCRIÇÃO E QUANTIDADE TOTAL DE LICENÇAS DE USO DE SOFTWARES A SEREM ADQUIRIDAS:

Item	Descrição	Quantidade de Licenças	Validade de mínima das licenças
1	PLATAFORMA DE ANTIVÍRUS GERENCIADO EM NUVEM PARA DESKTOP	850	12 meses
2	PLATAFORMA DE ANTIVÍRUS GERENCIADO EM NUVEM PARA SERVIDOR	7	12 meses

Deverão serem entregues as licenças em dois logins de acesso independentes, conforme quantidade de licenças abaixo:

Login 1	Descrição	Quantidade de Licenças	Validade de mínima das licenças
1	PLATAFORMA DE ANTIVÍRUS GERENCIADO EM NUVEM PARA DESKTOP	450	12 meses
2	PLATAFORMA DE ANTIVÍRUS GERENCIADO EM NUVEM PARA SERVIDOR	6	12 meses

Login 2	Descrição	Quantidade de Licenças	Validade de mínima das licenças
1	PLATAFORMA DE ANTIVÍRUS GERENCIADO EM NUVEM PARA DESKTOP	400	12 meses
2	PLATAFORMA DE ANTIVÍRUS GERENCIADO EM NUVEM PARA SERVIDOR	1	12 meses

3. CARACTERÍSTICAS GERAIS DA SOLUÇÃO

3.1 Todos os componentes que fazem parte da solução, de segurança para servidores, estações de trabalho deverão ser fornecidas por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes;

3.2 A console de monitoração e configuração deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas a fermentas para a monitoração e controle da proteção dos dispositivos;

3.3 A console de nuvem deve possuir o armazenamento de seus dados dentro do território nacional, garantindo conformidade e compliance com as leis locais como a LGPD, Instrução normativa 5 e NC-14 determinada pelo Banco Central;

3.4 A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional;

3.5 Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM;

3.6 Deve possuir capacidade de realizar a integração com soluções de firewalls para criar políticas automáticas em caso de ataques em massa nos computadores e servidores;

3.7 A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos;

3.8 Deve permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção.

3.9 Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos ou usuários;

3.10 A instalação deve ser feita via cliente específico por download da gerência central ou também via e-mail de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas;

3.11 Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;

3.12 Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;

3.13 Deve permitir exclusões de escaneamento para um determinado websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política.

3.14 A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs;

3.15 Atualização incremental, remota e em tempo real, da vacina dos Antivírus e do mecanismo de verificação (Engine) dos clientes;

3.16 Permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;

3.17 Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;

3.18 Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.

3.19 As mensagens geradas pelo agente deverão estar no idioma em português ou permitir a sua edição.

3.20 Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF;

3.21 Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

3.22 Possibilidade de exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status;

3.23 Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:

3.24 Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;

3.25 Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;

3.26 Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;

3.27 Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;

3.28 Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;

3.29 Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;

3.30 Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.

3.31 Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;

3.32 Deve fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares, procuradas palavras chaves ou informações confidenciais deve ser bloqueado o upload;

3.33 As portas de comunicação deverão ser configuráveis. A comunicação deverá permitir QoS para controlar a largura de banda de rede.

3.34 A solução deverá permitir a seleção da versão do software de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deverá ser transparente para os usuários finais.

3.35 O agente antivírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso à web;

3.36 Deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizadas soluções com senha única válida para todos os dispositivos;

3.37 Deve prover no endpoint a solução de HIPS (Host Instrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente;

3.38 Deve prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via web exploits;

3.39 Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria

estação de trabalho e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo;

3.40 O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio;

3.41 Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis seguras, CD, DVD, Blu-ray, floppy drives, interfaces de rede sem fio, modems, bluetooth, infravermelho, MTP (Media Transfer Protocol) tais como Blackberry, iPhone e Android smartphone e PTP (Picture Transfer Protocol) como câmeras digitais;

3.42 A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverá ser projetada para a fácil administração, supervisão e elaboração de relatórios dos endpoints e servidores;

3.43 Deverá possuir interface gráfica web, com suporte a língua portuguesa (padrão brasileiro);

3.44 A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do status de segurança;

3.45 Deverá fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção;

3.46 Deverá exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, etc.), e classificar os PCs em conformidade;

3.47 Uma vez que um problema seja identificado, deverá permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:

3.48 Proteger o dispositivo com a opção de início de uma varredura;

3.49 Forçar uma atualização naquele momento;

3.50 Ver os detalhes dos eventos ocorridos;

3.51 Executar verificação completa do sistema;

3.52 Forçar o cumprimento de uma nova política de segurança;

3.53 Mover o computador para outro grupo;

3.54 Apagar o computador da lista;

3.55 Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;

3.56 Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF;

3.57 Deverá conter vários relatórios para análise e controle dos usuários e endpoints. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints;

3.58 Fornece relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:

3.59 Nome do dispositivo;

3.60 Início da proteção;

3.61 Último usuário logado no dispositivo;

3.62 Último update;

3.63 Último escaneamento realizado;

3.64 Status de proteção do dispositivo;

3.65 Grupo a qual o dispositivo faz parte;

3.66 Permitir a execução manual de todos estes relatórios nos formatos CSV e PDF;

3.67 A console deve possuir métodos de verificação da saúde das configurações da console, possibilitando aos administradores descobrirem facilmente se existe alguma falha de configuração que pode facilitar a entrada de malwares e invasores no ambiente;

4. CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO

4.1 Características básicas do agente de proteção contra malwares:

4.2 Pré-execução do agente para verificar o comportamento malicioso e detectar malware desconhecido;

4.3 O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos;

4.4 O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;

4.5 O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

4.6 A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

4.7 Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

4.8 Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

4.9 Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

4.10 Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

4.11 Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

4.12 É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

4.13 Suportar máquinas com arquitetura 32-bit e 64-bit;

4.14 O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais, Microsoft Windows 10 e superior;

4.15 Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;

4.16 Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

5. FUNCIONALIDADE DE FIREWALL E DETECÇÃO E PROTEÇÃO DE INTRUSÃO (IDS\IPS) COM AS FUNCIONALIDADES:

5.1 Deverá possuir atualização periódica de novas assinaturas de ataque;

5.2 Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

5.3 Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidades conhecidas;

5.4 Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

5.5 Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

5.6 Deve possuir técnicas de proteção, que inclui:

5.7 Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

5.8 Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;

5.9 Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

5.10 Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

5.11 Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

6. FUNCIONALIDADE DE ANTIVÍRUS E ANTISPYWARE:

6.1.1 Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

6.1.2 Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

6.1.3 As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

6.1.4 Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

6.1.5 Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;

6.1.6 Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

6.1.7 Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

6.1.8 A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

6.1.9 Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

6.1.10 Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

6.1.11 Antivírus de Web (verificação de sites e downloads contra vírus);

6.1.12 Controle de acesso a sites por categoria;

6.1.13 Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

6.1.14 O Controle da Web deve controlar o acesso a sites impróprios, com categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

6.1.15 Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

6.1.16 Capacidade de verificar somente arquivos novos e alterados;

6.1.17 Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

7. **FUNCIONALIDADE DE DETECÇÃO PRÓ-ATIVA DE RECONHECIMENTO DE NOVAS AMEAÇAS:**

7.1.1 Funcionalidade de detecção de ameaças via técnicas de machine learning;

7.1.2 Funcionalidade de detecção de ameaças desconhecidas que estão em memória;

7.1.3 Capacidade de detecção, e bloqueio pró-ativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);

7.1.4 Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;

7.1.5 Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

8. **FUNCIONALIDADE DE PROTEÇÃO CONTRA RANSOMWARES:**

8.1.1 Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

8.1.2 Para estações de trabalho, dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

8.1.3 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;

8.1.4 A solução deverá prevenir ameaças e interromper que eles sejam executados em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.

8.1.5 Deverá possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de malware,

protegendo os endpoints de ameaças desconhecidas e vulnerabilidades *zero-day*.

8.1.6 Deve ser realizada a *detecção e o bloqueio de, pelo menos, as seguintes* técnicas de *exploit*:

8.1.6.1 DEP (*Data Execution Prevention*);

8.1.6.2 *Address Space Layout Randomization* (ASLR);

8.1.6.3 *Bottom Up ASLR*;

8.1.6.4 *Null Page*;

8.1.6.5 *Anti-HeapSpraying*;

8.1.6.6 *Dynamic Heap Spray*;

8.1.6.7 *Import Address Table Filtering (IAF)*;

8.1.6.8 *VTable Hijacking*;

8.1.6.9 *Stack Pivot and Stack Exec*;

8.1.6.10 *SEHOP*;

8.1.6.11 *Stack*-based ROP (*Return-Oriented Programming*);

8.1.6.12 *Control-Flow Integrity (CFI)*;

8.1.6.13 *Syscall*;

8.1.6.14 *WOW64*;

8.1.6.15 *Load Library*;

8.1.6.16 *Shellcode*;

8.1.6.17 *VBScript God Mode*;

8.1.6.18 *Application Lockdown*;

8.1.6.19 *Process Protection*;

8.1.6.20 *Network Lockdown*.

8.1.7 A solução deverá trabalhar silenciosamente na máquina do usuário e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de os arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve ser capaz de fazer a limpeza e remoção completa do ransomware na máquina do usuário.

8.1.8 Deverá fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real,

indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.

8.1.9 A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas a ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.

8.1.10 A console deverá apresentar *Dashboard* com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

9. **FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES E DISPOSITIVOS:**

9.1.1 Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;

9.1.2 Deverá atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

9.1.3 Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

9.1.4 Oferecer proteção para chaves de registro e controle de processos;

9.1.5 Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

9.1.6 Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

9.1.7 Deverá possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

9.1.8 Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

9.1.9 Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

9.1.10 As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

9.1.11 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

9.1.12 A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

9.1.13 Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

9.1.13.1 Permitir que todos os dispositivos do mesmo modelo;

9.1.13.2 Permitir que um único dispositivo com base em seu número de identificação único;

9.1.13.3 Permitir o acesso total;

9.1.13.4 Permitir acesso somente leitura;

9.1.14 Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

10. FUNCIONALIDADE DE PROTEÇÃO E PREVENÇÃO A PERDA DE DADOS:

10.1.1 Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

10.1.2 Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

10.1.3 Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

10.1.4 Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

10.1.4.1 Números de cartões de crédito;

10.1.4.2 Números de contas bancárias;

10.1.4.3 Números de Passaportes;

10.1.4.4 Endereços;

10.1.4.5 Números de telefone;

10.1.4.6 Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, entre outros;

10.1.4.7 Lista de e-mails;

10.1.4.8 Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, entre outros;

10.1.5 Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

10.1.6 Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

10.1.7 Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

10.1.8 Permitir o controle de dados para no mínimo os seguintes meios:

10.1.8.1 Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

10.1.8.2 Anexado no navegador (ao menos IE, Firefox e Chrome);

10.1.8.3 Anexado no cliente de mensagens instantâneas (ao menos Skype);

10.1.8.4 Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

11. CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA SERVIDORES:

11.1 CARACTERÍSTICAS BÁSICAS DO AGENTE DE PROTEÇÃO CONTRA MALWARES:

11.1.1 A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;

11.1.2 Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos;

11.1.3 O agente host deverá buscar algum sinal de malwares ativos e detectar malwares desconhecidos;

11.1.4 O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;

11.1.5 A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;

11.1.6 Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;

11.1.7 Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;

11.1.8 Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);

11.1.9 Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera, e bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

11.1.10 Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;

11.1.11 É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);

11.1.12 O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais abaixo:

11.1.12.1 Windows Server 2016, 2019 e 2022;
11.1.12.2 Amazon Linux;
11.1.12.3 Amazon Linux 2;
11.1.12.4 CentOS 7;
11.1.12.5 Debian 9;
11.1.12.6 Debian 10;
11.1.12.7 Oracle Linux 7;
11.1.12.8 Oracle Linux 8;
11.1.12.9 Red Hat Enterprise 7;
11.1.12.10 Red Hat Enterprise 8;
11.1.12.11 Red Hat Enterprise 9;
11.1.12.12 Ubuntu 20.04 LTS;

11.1.12.13 Ubuntu 22.04 LTS;

11.1.13 Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações;

11.1.14 Deve possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;

11.1.15 Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;

11.1.16 Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

11.1.17 Deve possuir funcionalidades de tecnologias conhecidas como CWPP – Cloud Workload Protection Plataform, permitindo que seja possível trazer funcionalidades de próxima geração para cargas de trabalho em nuvem, bem como containers, e afins;

11.1.18 A solução deve no mínimo, utilizar o modelo de sensores para containers, garantindo visibilidade e proteção de, no mínimo, estes tipos de ataques:

11.1.18.1 Escalação de privilégios dentro de containers;

11.1.18.2 Programas utilizando técnicas de mineração de criptomoedas;

11.1.18.3 Detecção de atacantes tentando destruir evidências de ambientes comprometidos (IOC – Indicator of compromise);

11.1.18.4 Detecção de funções internas do kernel que estão sendo adulteradas em um host;

11.1.19 A solução deve também se integrar a tecnologias de CSPM – Cloud Security Posture Management, tendo como objetivo trazer funcionalidades de análises integradas de CWPP e CSPM a fim de melhorar a visibilidade e resposta à incidentes em ambientes de nuvem públicas,

11.2 **FUNCIONALIDADE DE FIREWALL E DETECÇÃO E PROTEÇÃO DE INTRUSÃO (IDS\IPS) COM AS FUNCIONALIDADES:**

11.2.1 Possuir proteção contra exploração de buffer overflow;

11.2.2 Deverá possui atualização periódica de novas assinaturas de ataque;

11.2.3 Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo ou dinamicamente através do nome da aplicação.

11.2.4 Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;

11.2.5 Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.

11.2.6 Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.

11.2.7 Deverá possuir técnicas de proteção, que incluem:

11.2.7.1 Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;

11.2.7.2 Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;

11.2.7.3 Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

11.2.7.4 Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

11.2.7.5 Verificação de ameaças web avançadas**:** bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

11.3 **FUNCIONALIDADE DE ANTIVÍRUS E ANTISPYWARE:**

11.3.1 Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

11.3.2 Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

11.3.3 As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

11.3.4 Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

11.3.5 Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;

11.3.6 Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

11.3.7 Capacidade de detectar arquivos através da reputação dos mesmos;

11.3.8 Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

11.3.9 A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

11.3.10 Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

11.3.11 Deverá detectar tráfego de rede para comandar e controlar os servidores;

11.3.12 Proteger arquivos de documento contra ataques do tipo ransomwares;

11.3.13 Proteger que o ataque de ransomware seja executado remotamente;

11.3.14 Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante;

11.3.15 Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

11.3.16 Antivírus de Web (verificação de sites e downloads contra vírus);

11.3.17 Controle de acesso a sites por categoria;

11.3.18 Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

11.3.19 O Controle da Web deve controlar o acesso a sites impróprios, com categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

11.3.20 Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

11.3.21 Capacidade de verificar somente arquivos novos e alterados;

11.3.22 Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos

desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

11.3.23 Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças;

11.3.24 Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas;

11.4 **FUNCIONALIDADE DE PROTEÇÃO CONTRA RANSOMWARES:**

11.4.1 Deve dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;

11.4.2 Deve dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;

11.4.3 Deve 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;

11.5 **FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES E DISPOSITIVOS:**

11.5.1 Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;

11.5.2 Deverá atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possa ser liberada ou bloqueada;

11.5.3 Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

11.5.4 Oferecer proteção para chaves de registro e controle de processos;

11.5.5 Proibir através de política a inicialização de um processo ou aplicativo baseado em nome ou no hash do arquivo;

11.5.6 Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

11.5.7 Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

11.5.8 Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

11.5.9 Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;

11.5.10 As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

11.5.11 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

11.5.12 A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;

11.5.13 Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

11.5.13.1 Permitir que todos os dispositivos do mesmo modelo;

11.5.13.2 Permitir que um único dispositivo com base em seu número de identificação único;

11.5.13.3 Permitir o acesso total;

11.5.13.4 Permitir acesso somente leitura;

11.5.14 Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

11.6 FUNCIONALIDADE DE PROTEÇÃO E PREVENÇÃO A PERDA DE DADOS:

11.6.1 Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

11.6.2 Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações

confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

11.6.3 Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

11.6.4 Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:

11.6.4.1 Números de cartões de crédito;

11.6.4.2 Números de contas bancárias;

11.6.4.3 Números de Passaportes;

11.6.4.4 Endereços;

11.6.4.5 Números de telefone;

11.6.4.6 Códigos postais definidas por países como Brasil, França, Inglaterra, Alemanha, EUA, entre outros;

11.6.4.7 Lista de e-mails;

11.6.4.8 Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, entre outros;

11.6.5 Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

11.6.6 Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.

11.6.7 Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

11.6.8 Permitir o controle de dados para no mínimo os seguintes meios:

11.6.8.1 Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);

11.6.8.2 Anexado no navegador (ao menos IE, Firefox e Chrome);

11.6.8.3 Anexado no cliente de mensagens instantâneas (ao menos Skype);

11.6.8.4 Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

11.7 CAPACIDADE TÉCNICA:

11.7.1 Atestado de Capacidade Técnica demonstrando que a proponente forneceu **o serviço**, para pessoa física ou jurídica de direito público ou privado, e realizou a instalação, configuração e suporte técnico de solução de **antivírus** igual ou superior com o objeto deste termo de referência.

12. SUPORTE TÉCNICO, TREINAMENTO E MANUTENÇÃO:

12.1.1 Suporte Técnico e manutenção oferecidos pelo fabricante do software.

12.1.2 A contratada, caso não seja o próprio fabricante, deve possuir contrato de suporte técnico para atendimento ilimitado junto ao fabricante do produto oferecido, a fim de garantir o serviço prestado;

12.1.3 Serviços de suporte especializado em segurança da informação para instalação, configuração e suporte ao funcionamento da solução antimalware. O suporte será em regime de, no mínimo, 8 horas x 5 dias por semana(horário comercial);

12.1.4 Suporte técnico telefônico no idioma português Brasil direto com o fabricante do produto e a contratada;

12.1.5 Com direito a atualizações de assinaturas e software, e suporte técnico ilimitado (via e-mail e telefone), sem custo adicional, pelo período de contratação do software antivírus a contar do recebimento das licenças de uso pela Prefeitura;

12.1.6 O telefonema para o suporte técnico remoto deverá ser atendido por técnico devidamente capacitado para interpretar e, eventualmente resolver ou contatar os recursos necessários para a resolução do problema em regime de, no mínimo, 8 horas x 5 dias por semana.

12.1.7 Fornecimento de vacina para novos vírus no prazo máximo de 48 horas a partir do registro de ocorrência feito pela Prefeitura.

12.1.8 O tempo máximo de 3 (três) dias úteis para resolução de suporte técnico, quando não para vacina.

12.1.9 Deverá ser indicado o site do fabricante para download autorizado do produto e dos manuais.

12.1.10 Demonstração do software para avaliação técnica:

12.1.11 A SEPPTI (Seção Especial de Políticas Públicas de Tecnologia da Informação) poderá solicitar do fornecedor, durante o período de julgamento da proposta, uma demonstração das características técnicas do software oferecido, para avaliação a ser efetuada por equipe técnica da Prefeitura. O software para

avaliação deverá ser entregue ao Departamento de Tecnologia, Informação em até 3 (três) dias úteis após o recebimento, pelo fornecedor, da solicitação da Prefeitura.

12.1.12 Durante o período de avaliação, o fornecedor deverá prestar os esclarecimentos e suporte que venham a ser solicitados pela equipe técnica da Prefeitura.

12.1.13 O aceite técnico da SEPPTI (Seção Especial de Políticas Públicas de Tecnologia da Informação) será dado quando for constatado o atendimento a todos os requisitos do software.

12.1.14 Os serviços de consultoria e treinamento deverão ser prestados por técnico(s) qualificado(s) do fornecedor a partir de cronograma a ser definido com a equipe técnica da SEPPTI (Seção Especial de Políticas Públicas de Tecnologia da Informação), e serão realizados nas dependências da Prefeitura ou por meio de web conferência.

12.1.15 A contratada deverá emitir certificado de participação para cada participante, constando nome do curso, carga horária, data da realização e o nome do treinando;

12.1.16 Todo material didático de apoio necessário ao desenvolvimento dos cursos, como manuais, esquemas e apostilas deverá ser fornecido pela contratada a todos os participantes, individualmente, no início de cada curso e deverão estar preferencialmente escritos em língua portuguesa;

12.1.17 O treinamento deverá contemplar em seu conteúdo, no mínimo:

12.1.18 Funcionalidades gerais do software antimalware (antivírus) e demais funcionalidades;

12.1.19 Instalação do console de gerenciamento em ambiente servidor, se for o caso;

12.1.20 Instalação do antivírus nas estações de trabalho através da console, stand alone, script de instalação ou via GPO utilizando o Active Directory;

12.1.21 Criação e aplicação de políticas de restrições e/ou exceções em estações de trabalho e/ou servidores, individualmente ou em grupos.

12.1.22 O treinamento deverá ter carga horária mínima de 8 (oito) horas,

12.1.23 O cronograma para realização da consultoria técnica e do treinamento será definido a partir de entendimentos prévios com a equipe técnica da Prefeitura.

12.1.24 Para a execução dos serviços de consultoria e treinamento, o fornecedor deverá apresentar à Prefeitura, por ocasião do início dos trabalhos, certificado(s) de

qualificação emitido(s) pela empresa fabricante do antivírus em nome do(s) técnico(s) que será(ão) responsável(veis) pela instalação, configuração e implementação de gerenciamento do software.