TERMO DE REFERÊNCIA

1. OBJETO

1.1 Contratação de empresa para fornecimento de licenças de solução de segurança antivírus para uso no parque tecnológico da autarquia.

2. JUSTIFICATIVA DA CONTRATAÇÃO

2.1 A aquisição das licenças de software antivírus tem o objetivo prevenir a contaminação por vírus, malwares e suas variantes bem como ameaças cibernéticas distintas nos computadores da autarquia que podem colocar em risco o sigilo, a integridade e disponibilidade das informações.

2.2 Com o grande volume de utilização e com o crescimento da utilização de e-mails e acesso a páginas de internet a utilização de um software de antivírus é necessária para fornecer um mínimo de segurança à infraestrutura de rede de computadores.

2.3 A aquisição propõe uma maior proteção aos computadores e servidores, resguardando problemas que podem prejudicar os serviços executados.

2.4 Assim, a aquisição das licenças de antivírus é considerada imprescindível para garantir a disponibilidade, integridade e confiabilidade dos dados e continuidade das atividades da Sama.

3. ESPECIFICAÇÕES DOS ITENS

Item	Descrição	Quantidade de Licenças	Validade mínima das licenças
1	Fornecimento de licenças de uso de solução corporativa de antivírus/anti-exploit/anti-ransomware para estações de trabalho com gerência em nuvem.	28	12 meses
2	Fornecimento de licenças de uso de solução corporativa de antivírus/anti-exploit/anti-ransomware para servidores com gerência em nuvem.	14	12 meses

4. CARACTERÍSTICAS GERAIS DA SOLUÇÃO

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

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

4.3 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;

4.4 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 em diferentes níveis, como por exemplo, alta, média e informacional, entre outras que a solução possa apresentar;

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

4.6 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;

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

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

4.9 Deve possuir a possibilidade de aplicar regras diferenciadas baseadas em grupos ou usuários;

4.10 A instalação deve ser feita via cliente específico por download da central de gerência. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas;

4.11 A console deve 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;

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

4.13 Deve permitir exclusões de escaneamento para determinados websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política;

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

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

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

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

4.18 Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados;

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

4.20 Permitir a exportação dos relatórios gerenciais para, pelo menos, os formatos CSV e PDF;

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

4.22 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;

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

4.23.1 Detalhamento de quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;

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

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

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

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

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

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

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

4.25 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, procura de palavras chaves ou informações confidenciais. Deve ser bloqueado o upload ou removida a informação confidencial antes do envio do arquivo;

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

4.27 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.

4.28 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 ((Potentially Unwanted Application)), adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso à web;

4.29 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;

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

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

4.32 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;

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

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

4.35 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 endpoint e servidores;

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

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

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

4.39 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;

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

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

4.40.2 Forçar uma atualização naquele momento;

4.40.3 Ver os detalhes dos eventos ocorridos;

4.40.4 Executar verificação completa do sistema;

4.40.5 Forçar o cumprimento de uma nova política de segurança;

4.40.6 Mover o computador para outro grupo;

4.40.7 Apagar o computador da lista;

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

4.42 Gravar um log de auditoria seguro, que monitore a atividade na console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses;

4.43 Deverá permitir exportar o relatório de logs de auditoria pelo menos nos formatos CSV e PDF;

4.44 Deve 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;

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

4.45.1 Nome do dispositivo;

4.45.2 Início da proteção;

4.45.3 Último usuário logado no dispositivo;

4.45.4 Último update;

4.45.5 Último escaneamento realizado;

4.45.6 Status de proteção do dispositivo;

4.45.7 Grupo ao qual o dispositivo faz parte;

4.46 Permitir a execução manual de todos estes relatórios pelo menos nos formatos CSV e PDF;

4.47 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;

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

5.1 Características básicas do agente de proteção contra malwares:

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

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

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

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

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

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

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

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

5.10 Deve proteger os navegadores IE, Edge, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

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

5.12 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);

5.13 Suportar máquinas com arquitetura 32-bit e 64-bit, (exceto para Windows 11 que não há opção de 32bits);

5.14 O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais Microsoft Windows 7, 8.1, 10 e 11;

5.15 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;

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

6. FUNCIONALIDADE DE FIREWALL E DETECÇÃO E PROTEÇÃO DE INTRUSÃO (IDS\IPS)

6.1 Deverá possuir atualização periódica de novas assinaturas de ataque;

6.2 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;

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

6.4 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;

6.5 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;

6.6 Deve possuir técnicas de proteção, que incluam:

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

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

6.6.3 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;

6.6.4 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);

6.6.5 Verificação de ameaças web avançadas: bloqueando 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;

7. FUNCIONALIDADE DE ANTIVÍRUS E ANTISPYWARE

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

7.2 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;

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

7.4 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;

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

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

7.7 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;

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

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

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

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

7.12 Controle de acesso a sites por categoria;

7.13 Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Edge, Firefox, Safari, 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 seja possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites;

7.14 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;

7.15 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;

7.16 Capacidade de verificar somente arquivos novos e alterados;

7.17 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.

8. FUNCIONALIDADE DE DETECÇÃO PRÓ-ATIVA DE RECONHECIMENTO DE NOVAS AMEAÇAS

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

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

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

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

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

9. FUNCIONALIDADE DE PROTEÇÃO CONTRA RANSOMWARES

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

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

9.3 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;

9.4 A solução deverá prevenir ameaças e interromper que elas sejam executadas em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas;

9.5 Deve 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.

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

9.6.1 DEP (Data Execution Prevention);
9.6.2 Address Space Layout Randomization (ASLR);
9.6.3 Bottom Up ASLR;
9.6.4 Null Page;
9.6.5 Anti-HeapSpraying;
9.6.6 Dynamic Heap Spray;
9.6.7 Import Address Table Filtering (IAF);
9.6.8 VTable Hijacking;
9.6.9 Stack Pivot and Stack Exec;
9.6.10 SEHOP;
9.6.11 Stack-based ROP (Return-Oriented Programming);
9.6.12 Control-Flow Integrity (CFI);
9.6.13 Syscall;
9.6.14 WOW64;
9.6.15 Load Library;
9.6.16 Shellcode;
9.6.17 VBScript God Mode;
9.6.18 Application Lockdown;
9.6.19 Process Protection;

9.6.20 Network Lockdown.

9.7 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 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;

9.8 Deve 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;

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

9.10 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.

10. SOLUÇÃO DE ENDPOINT DETECTION AND RESPONSE (EDR)

10.1 A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

10.2 Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta à nuvem de inteligência do fabricante;

10.3 Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio;

10.4 Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

10.4.1 Detalhes do processo, como nome, hash, hora e data da detecção e remediação;

10.4.2 Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

10.4.3 Resultado da análise do arquivo suspeito pela funcionalidade de Machine Learning;

10.4.4 Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado**;**

10.5 A solução de EDR deverá ser integrada ao agente de antivírus a ser instalado com um agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

10.6 O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

10.7 Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

10.8 Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

10.9 Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

10.10 Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

10.11 Deve possibilizar o agendamento de consultas (queries);

10.12 Deve reter os dados no Data Lake por no mínimo 7 dias.

11. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES E DISPOSITIVOS

11.1 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;

11.2 Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas;

11.3 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;

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

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

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

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

11.8 Gerenciar o uso de dispositivos de armazenamento USB (ex.: pen-drives e HDs externos);

11.9 Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;

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

11.11 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;

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

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

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

11.13.2 Permitir todos os dispositivos do mesmo modelo;

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

11.13.4 Permitir o acesso total;

11.13.5 Permitir acesso somente leitura;

11.13.6 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.

12. FUNCIONALIDADE DE PROTEÇÃO E PREVENÇÃO À PERDA DE DADOS

12.1 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;

12.2 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);

12.3 Possibilitar o bloqueio, somente registrar o evento na console de administração, ou perguntar ao usuário se ele(a) realmente quer transferir o arquivo identificado como sensível;

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

12.4.1 Números de cartões de crédito;

12.4.2 Números de contas bancárias;

12.4.3 Números de passaportes;

12.4.4 Endereços;

12.4.5 Números de telefone;

12.4.6 Códigos postais definidos por países;

12.4.7 Lista de e-mails;

12.4.8 Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários etc.;

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

12.6 Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo;

12.7 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;

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

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

12.8.2 Anexado no navegador (ao menos IE, Edge, Firefox e Google Chrome);

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

12.8.4 Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD).

13. CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA SERVIDORES

13.1 Características básicas do agente de proteção contra malwares:

13.2 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;

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

13.4 O agente host deve buscar algum sinal de malwares ativos e detectar malwares desconhecidos;

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

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

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

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

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

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

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

13.12 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);

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

13.13.1 Windows Server 2025;
13.13.2 Windows Server 2019;
13.13.3 Windows Server 2016;
13.13.4 Windows Server 2012 R2 (64 bits);
13.13.5 Windows Server 2012 (64 bits);
13.13.6 Amazon Linux;
13.13.7 Amazon Linux 2;
13.13.8 CentOS 7;
13.13.9 Debian 10;
13.13.10 Oracle Linux 7;
13.13.11 Oracle Linux 8;
13.13.12 Red Hat Enterprise 7;
13.13.13 Red Hat Enterprise 8;
13.13.14 Red Hat Enterprise 9;
13.13.15 SUSE Linux Enterprise Server 12;
13.13.16 SUSE Linux Enterprise Server 15;
13.13.17 Ubuntu 20.04 LTS;
13.13.18 Ubuntu 22.04 LTS;

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

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

13.16 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;

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

13.18 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;

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

13.19.1 Escalação de privilégios dentro de containers;

13.19.2 Programas utilizando técnicas de mineração de criptomoedas;

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

13.19.4 Detecção de funções internas do kernel que estejam sendo adulteradas em um host;

13.20 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.

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

14.1 Possuir proteção contra exploração de buffer overflow;

14.2 Deverá possui atualização periódica de novas assinaturas de ataque;

14.3 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;

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

14.5 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;

14.6 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;

14.7 Deve possuir técnicas de proteção, que inclui:

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

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

14.7.3 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;

14.7.4 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);

14.7.5 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;

15. FUNCIONALIDADE DE ANTIVÍRUS E ANTISPYWARE:

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

15.2 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;

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

15.4 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;

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

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

15.7 Capacidade de detectar arquivos através da reputação dos mesmos;

15.8 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;

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

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

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

15.12 Proteger arquivos de documento contra-ataques do tipo ransomwares;

15.13 Proteger que o ataque de ransomware seja executado remotamente;

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

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

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

15.17 Controle de acesso a sites por categoria;

15.18 Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Edge, Firefox, Safari, 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;

15.19 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;

15.20 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;

15.21 Capacidade de verificar somente arquivos novos e alterados;

15.22 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;

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

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

16. FUNCIONALIDADE DE PROTEÇÃO CONTRA RANSOMWARES:

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

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

16.3 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;

17. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES E DISPOSITIVOS:

17.1 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;

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

17.3 Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões;

17.4 Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

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

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

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

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

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

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

17.11 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;

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

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

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

17.14.1 Permitir que todos os dispositivos do mesmo modelo;

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

17.14.3 Permitir o acesso total;

17.14.4 Permitir acesso somente leitura;

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

18. FUNCIONALIDADE DE PROTEÇÃO E PREVENÇÃO A PERDA DE DADOS

18.1 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;

18.2 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);

18.3 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;

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

18.4.1 Números de cartões de crédito;

18.4.2 Números de contas bancárias;

18.4.3 Números de passaportes;

18.4.4 Endereços;

18.4.5 Números de telefone;

18.4.6 Códigos postais definidas por países;

18.4.7 Lista de e-mails;

18.4.8 Informações pessoais, corporativas e financeiras referentes especificamente ao Brasil, como CPF, RG, CNH, CNPJ, dados bancários, etc;

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

18.6 Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo;

18.7 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;

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

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

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

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

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

19. SOLUÇÃO DE ENDPOINT DETECTION AND RESPONSE (EDR)

19.1 A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;

19.2 Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante;

19.3 Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.

19.4 Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:

19.4.1 Detalhes do processo, como nome, hash, hora e data da detecção e remediação;

19.4.2 Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

19.4.3 Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;

19.4.4 Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;

19.5 A solução de EDR deverá ser integrada ao agente de antivírus a ser instalado com um agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

19.6 O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;

19.7 Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;

19.8 Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;

19.9 Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;

19.10 Deve ter acesso a recurso de Data Lake que armazene informações críticas de endpoints e servidores, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

19.11 Deve possibilizar o agendamento de consultas;

19.12 Deve reter os dados no Data Lake por no mínimo 7 dias.

20. SOLUÇÃO DE EXTENDED DETECTION AND RESPONSE (XDR)

20.1 Deve possuir Data Lake que armazene informações críticas de endpoints e servidores, mas também incorporando dados de outras soluções de segurança como firewalls, e-mail gateways, public cloud e mobile, permitindo o acesso aos dados sobre atividades mesmo quando o dispositivo correspondente está offline ou foi descontinuado;

20.2 Deve possuir recurso de pesquisa estruturada em banco de dados compatível com SQL, ou similar;

20.3 Deve disponibilizar recurso de pesquisa para comparar os indicadores de comprometimento de várias fontes de dados para identificar rapidamente um ataque suspeito;

20.4 Deve utilizar detecções de ATP e IPS do firewall para investigar endpoints suspeitos;

20.5 Deve disponibilizar pontos de aplicação que permitem a executar ações, como colocar em quarentena um endpoint comprometido, bloquear o tráfego de rede ou remover malware;

20.6 Deve possuir sensores que forneçam telemetria de diferentes aspectos da infraestrutura de TI, capazes de identificar dispositivos não gerenciados e desprotegidos em todo o ambiente da organização;

20.7 Deve possibilitar o agendamento de consultas (queries) cíclicas no Data Lake para identificação de IoCs em execuções antecipadas;

20.8 Deve permitir a integração via APIs com sistemas e fluxos de trabalhos já existentes;

20.9 Deve reter os dados no Data Lake por no mínimo 30 dias.

20.10 O XDR deve permitir integração com sistemas de terceiros, no mínimo, tecnologias como Office 365 e produtos de CSPM para visibilidade e correlação de eventos em ambientes de Cloud como Azure, AWS e Google Cloud;

20.11 A console do XDR deve correlacionar os dados recebidos e armazenados no Data Lake e gerar evidências de ataques ou eventos suspeitos existentes dentro do ambiente;

20.12 Tais detecções e evidências devem conter todos os detalhes do evento, bem como uma análise do próprio fabricante sobre a classificação de risco de tal evento;

20.13 Deve possibilitar também que investigações sejam realizadas a partir destes eventos, coletando dados e executando consultas dentro do Data Lake ou nos próprios dispositivos a fim de coletar mais evidências para determinar a realidade do ataque presente na console;

20.14 Deve possuir console para gerenciamento de investigações, podendo adicionar de forma automática ou manual, diversos eventos e detecções encontradas na console;

20.15 A console de gerenciamento de investigações deve permitir atribuir analistas que acompanharão a investigação.

21. INTEGRAÇÕES

21.1 Deve disponibilizar integração com ferramentas de NDR (Network Detect and Response) do próprio fabricante, podendo ser entregue via appliance virtual compatível com ESXI e Hyper-V minimamente ou Hardware próprio, não sendo aceito equipamentos do tipo PC;

21.2 Deve ser compatível com integrações de terceiros com as seguintes categorias com no mínimo os seguintes fabricantes:

21.2.1 Firewalls:

- Check Point;
- Palo Alto;
- Fortinet;
- Cisco;
- SonicWall.

21.2.2 Endpoints:

- Microsoft;
- CrowdStike;
- McAfee;
- SentinelOne;
- Check Point;
- Trend Micro;
- Malwarebytes;
- BalckBerry;
- Palo Alto Cortex XDR.

21.2.3 Provedores de identidade:

- Microsoft Azure IDP, ATA;
- Okta;
- Duo.

21.2.4 Plataformas de e-mails:

- Microsoft 365;
- Mimecast;
- Proofpoint.

21.2.5 Cloud SaaS:

- AWS;
- Azure;
- Google Cloud;
- Orca Security;
- Prisma Cloud.

21.2.6 Network:

- Darktrace;
- Forcepoint.

21.3 As integrações de terceiros poderão ser via API ou envio de Syslogs;

21.4 A solução deve fornecer ferramenta para a coleta de telemetria de eventos de terceiros que não usam API entregando uma imagem de sistema do tipo .OVA para uso em virtualizador;

21.5 O fabricante deve disponibilizar através de um website a lista de tecnologias e fabricantes suportados, para eventuais consultas.

22. IMPLANTAÇÃO DA SOLUÇÃO

22.1 A implantação da solução deverá ser realizada em conjunto pela equipe técnica da contratada com a equipe técnica da Sama;

22.2 A contratada deverá dispor de equipe técnica certificada na solução (com apresentação de certificados técnicos emitidos pelo fabricante ou entidade autorizada por este para esta finalidade);

22.3 Todas as políticas e regras existentes na solução atualmente em uso (Symantec Endpoint Protection) deverão ser migradas e/ou replicadas para a nova solução, respeitando-se as características de cada solução;

22.4 O serviço de implantação deverá ser realizado em horário comercial, sendo de segunda à sexta-feira, entre às 9h00min e às 17h00min, devendo ser tratado junto à equipe técnica da Sama caso haja a necessidade da realização de algum trabalho fora do horário comercial;

23. SUPORTE TÉCNICO

23.1 A contratada deverá prover suporte técnico na solução durante o período de vigência das licenças (12 meses);

23.2 O suporte técnico deverá estar disponível em horário comercial, sendo de segunda à sexta-feira, entre às 8h00min e às 17h00min;

23.3 A contratada deverá dispor de plataforma própria para realização de abertura e acompanhamento de chamados técnicos;

23.4 Após abertura de chamado técnico deverá haver resposta em até 2 horas.

24. TREINAMENTO

24.1 A contratada deverá prover treinamento prático na solução para 1 (um) técnico indicado pela Sama;

24.2 O treinamento deverá abordar todas as funções presentes na solução, como gerenciamento do dashboard, emissão de relatórios, instalação, configuração de regras e políticas, solução de problemas comuns etc.;

24.3 O treinamento deverá ser ministrado em horário comercial, devendo ser tratado junto à equipe técnica da Sama caso haja a necessidade da realização fora do horário comercial.

25. OBRIGAÇÕES DA CONTRATADA

25.1 Fornecer as licenças contratadas em sua integralidade;

25.2 Fornecer todos os serviços solicitados como implantação, treinamento e suporte técnico;

25.3 Realizar a reconfiguração de qualquer agente/política que a equipe técnica da Sama identifique estar em desacordo com o pedido ou em mal funcionamento, sem ônus algum para a Autarquia.

26. OBRIGAÇÕES DA CONTRATANTE

26.1 Disponibilizar informações necessárias para garantir a compatibilidade dos sistemas e softwares fornecidos;

26.2 Fornecer a infraestrutura necessária à implantação da solução;

26.3 Realizar o pagamento conforme estipulado no edital.

27. PRAZO E LOCAL DE ENTREGA

27.1 Prazo de entrega: até 15 (quinze) dias corridos após emissão do pedido de compras.

27.2 Local de entrega: Av. Washington Luiz, 2.923 – Vl. Magini – Mauá – SP – 09390-140 e/ou através do e-mail ti@pmmsama.sp.gov.br no caso de licenças apenas em formato digital.

28. CONDIÇÕES DE PAGAMENTO

28.1 Pagamento por boleto ou transferência até 10 (dez) dias após a entrega dos itens e serviços.

29. FORMA DE JULGAMENTO

29.1 Critério: menor preço global;

29.2 Proposta deve incluir todos os itens e custos previstos.

30. FUNDAMENTAÇÃO LEGAL

2.1 Lei Federal nº 14.133/2021 (Nova Lei de Licitações e Contratos), e normas correlatas.

31. CONSIDERAÇÕES FINAIS

31.1 Este Termo de Referência visa subsidiar a instrução do processo licitatório para aquisição de licenças de software de proteção antivírus, atendendo aos princípios da legalidade, impessoalidade, eficiência e economicidade, conforme a legislação vigente.