PREFEITURA MUNICIPAL DE SANTA MARIA/RS

Termo de Referência 55/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
55/2026	988841-PREFEITURA MUNICIPAL DE SANTA MARIA /RS	SABRINA MEDIANEIRA DA SILVA AVILA	04/11/2026 10:53 (v 0.12)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC		55/2026

1. Definição do Objeto

1.1 Contratação de empresa especializada para renovação e acréscimo de licenças do software de proteção Kaspersky, conforme especificações constantes neste Termo de Referência.

ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE
Renovação de Licença de Antivírus Kaspersky para Estação de Trabalho	24333	Unidade	2.000
Renovação de Licença de Antivírus Kaspersky para Ambiente Virtualizado	24333	Unidade	200
Serviço de Instalação e Configuração da Solução Antivírus, com Treinamento "Hands-On" da Solução de Antivírus	3840	Serviço	1

1.2. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.3. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.4. O prazo de vigência da contratação é de 60 (sessenta) meses, admitida sua prorrogação na forma da Lei nº 14.133/2021. Os itens 1 e 2 poderão ser renovados mediante conveniência e necessidade da Contratante.

2. Justificativa

Considerando que a disponibilidade de uma solução de antivírus corporativo é imprescindível para garantir a segurança da informação e a integridade de todo o parque tecnológico do Município de Santa Maria;

Considerando que o investimento em segurança digital não representa um mero custo de Tecnologia da Informação, mas sim um mecanismo de continuidade de negócios, essencial para mitigar riscos de paralisação de sistemas vitais, assegurar a estrita conformidade com as exigências da Lei Geral de Proteção de Dados (LGPD), proteger o patrimônio digital contra vazamentos e dotar a equipe técnica da capacidade de centralizar, monitorar e responder a incidentes antes que se convertam em crises financeiras ou de imagem pública;

Considerando as competências institucionais da Superintendência de Tecnologia da Informação em manter em pleno funcionamento os diversos serviços municipais essenciais prestados ao cidadão, tais como prontuários médicos na rede de saúde, sistemas de assistência e dados sociais, e o cadastro imobiliário, histórico este respaldado pelo uso de soluções centralizadas corporativas desde 2015, as quais mantiveram o parque de máquinas e os dados públicos seguros e livres de intercorrências graves;

Considerando que a área de Tecnologia da Informação, em especial a camada de segurança cibernética, passa por rápida e constante evolução, exigindo a atualização dos mecanismos de proteção ao longo dos anos para fazer frente ao surgimento de ameaças digitais cada vez mais complexas;

Considerando que os Contratos nº 45/2015 e nº 23/2020 previam a contratação de solução de antivírus tradicional do tipo **EPP (*Endpoint Protection Platform*)**, cuja eficácia é limitada à detecção por assinaturas de ameaças já conhecidas, mostrando-se insuficiente contra ataques inéditos (*Dia Zero*); e que referida tecnologia evoluiu para o modelo **EDR (*Endpoint Detection and Response*)**, focado no monitoramento comportamental detalhado, histórico de processos, conexões e isolamento preventivo de ativos;

Considerando que o estado da arte atual consolidou a tecnologia **XDR (*Extended Detection and Response*)**, que expande a inteligência do EDR ao integrar e correlacionar dados não apenas dos terminais, mas também da rede, nuvem e gerenciadores de identidade (como o *Active Directory*), otimizando drasticamente o tempo de resposta a incidentes sem a dependência exclusiva de vacinas prévias;

Considerando a diretriz iniciada no Contrato nº 831/2023 para a adoção do formato SaaS (*Software as a Service*) na camada XDR, visa-se consolidar este modelo tecnológico avançado por meio da atualização, migração e renovação das licenças da fabricante Kaspersky, cuja a equipe técnica já possui conhecimento prévio do funcionamento;

DA JUSTIFICATIVA PARA O LOTE ÚNICO

Considerando que o objeto contempla componentes de uma mesma solução de segurança, abrangendo licenciamento, monitoramento gerenciado, instalação e configuração, optou-se pelo agrupamento em lote único, visando assegurar a integração funcional entre os componentes, a centralização da gestão e a uniformidade dos procedimentos de suporte e atendimento.

O agrupamento também busca concentrar a responsabilidade pela implantação e pelo funcionamento integrado da solução em uma única contratada, reduzindo possíveis conflitos de responsabilidade técnica e dificuldades de integração entre diferentes fornecedores. Dessa forma, entende-se que a contratação conjunta atende melhor às necessidades operacionais da Administração.

DA JUSTIFICATIVA PARA A INDICAÇÃO DE MARCA (PADRONIZAÇÃO)

Considerando que o Município adquiriu as licenças *Kaspersky Endpoint Security for Business Versão Select* e *Kaspersky Hybrid Cloud Security* por meio do Contrato nº 23/2020, e que a solução desempenhou suas funções durante todo o período contratual com estabilidade, alta taxa de fidedignidade e excelente desempenho de hardware (mostrando-se leve para as estações de trabalho no cotidiano operacional);

Considerando que a manutenção da marca assegura a **padronização tecnológica** da solução de segurança, evitando custos invisíveis com novos treinamentos da equipe técnica, reinstalações massivas em centenas de computadores da rede municipal e riscos de incompatibilidade com os sistemas governamentais legados vigentes;

Considerando, por fim, que a pesquisa de preços realizada no mercado técnico indica que a renovação/atualização com foco na marca já adotada proporciona uma **redução de até 26% nos custos** para um horizonte contratual de 5 (cinco) anos, se comparada à aquisição do zero de novas subscrições concorrentes de tecnologia XDR equivalente;

A indicação da marca não implica exclusividade de fornecedor, sendo admitida a participação de empresas revendedoras ou representantes que comprovem o atendimento integral aos requisitos técnicos e comerciais estabelecidos neste Termo de Referência.

OPTOU-SE pela indicação e renovação das licenças da marca **Kaspersky**, medida que atende plenamente aos princípios da economicidade, da eficiência administrativa e do interesse público na proteção dos ativos digitais do Município de Santa Maria.

3. Entrega

3.1 A contratada deve efetuar a entrega das chaves de ativação de forma online através da internet ou enviá-las por e-mail (sti@santamaria.rs.gov.br) no prazo não superior a 15 (quinze) dias corridos, contados do recebimento da Nota de Empenho.

3.2 O serviço de instalação e configuração deverá ser concluído até o dia 31/12/2026.

3.3 A validade das licenças será contada a partir de 04/01/2027.

3.4 Etapas do Processo de Configuração e Instalação

Etapa	Descrição	Início	Responsável
1	Reunião de Alinhamento	Em até 10 dias úteis da emissão da Nota de Empenho	Equipe técnica da Contratante e da Contratada
2	Envio das Características do Servidor Centralizador	Em até 5 dias úteis da Etapa 1	Contratada
3	Disponibilização do Acesso ao Servidor Centralizado	Em até 10 dias úteis da Etapa 2	Contratante
4	Configuração e Instalação das Licenças	Até 31/12/2026	Contratada
5	Treinamento	Até 31/12/2026	Equipe técnica da Contratante e da Contratada
6	Início da Vigência das Licenças (item 1 e 2)	04/01/2027	Equipe técnica da Contratante e da Contratada
7	Início do Suporte	A partir de 04/01/2027	Contratada

3.4.1 Os contatos para agendamentos e alinhamentos deverão ser centralizados no email sti@santamaria.rs.gov.br.

4. Garantia

4.1 O prazo de garantia, suporte técnico, atualização e manutenção (upgrade e update) da solução de antivírus será é de no mínimo 60 (sessenta) meses, ou seja, durante toda a vigência do contrato.

4.2 A garantia incluirá, além da prestação de serviços de suporte técnico, a manutenção e atualização da solução sem qualquer ônus para a Contratante.

4.3 A Contratada será responsável pela disponibilização de atualizações (updates e upgrades) da solução durante toda a vigência contratual, sem custos adicionais para a Contratante. Após a conclusão dos serviços de instalação, configuração e treinamento, a administração operacional da plataforma ficará sob responsabilidade da equipe técnica da Contratante, permanecendo a Contratada responsável pela prestação do suporte técnico previsto neste Termo de Referência.

5. Descrição da Solução

5.1 Características do Módulo Centralizador

5.1.1 O servidor principal de gerência da solução de antivírus será o responsável por gerenciar e distribuir as atualizações lançadas pelo fabricante da SOLUÇÃO DE ANTIVÍRUS entre os servidores secundários de atualizações do parque computacional, que devem ser os responsáveis por fornecer as atualizações aos computadores localizados em sua própria rede.

5.1.2 Desta forma, qualquer servidor secundário de atualização com a licença adquirida no conjunto da solução e que se encontre conectado na rede da PMSM deve solicitar e receber as atualizações da solução de antivírus diretamente do servidor principal de gerência. Os computadores da rede local dos servidores secundários de atualizações, localizados nas unidades remotas ou REDE MPLS, devem receber exclusivamente as atualizações através do repositório desses servidores.

5.1.3 O módulo de gerência principal da solução (Servidor Principal de Gerência da Solução) fará todo o controle da solução de antivírus através de único console central de gerenciamento. A equipe técnica da PMSM será a responsável pela gestão da solução.

5.1.4 Será disponibilizado pela Contratante um servidor virtualizado para instalação do módulo centralizador da solução, as características de hardware deverão ser apresentadas pela Contratada na reunião de alinhamento da entrega da Solução, podendo ser disponibilizado ainda licença de Windows Server 2019 ou distribuições Linux.

5.2 Características mínimas para a Solução de Antivírus item 1 e 2

5.2.1 Deverão ser renovadas e atualizadas as 2.000 licenças da Solução de Antivírus Kaspersky adquiridas no Contrato 23/2020, para a versão Kaspersky NEXT XDR Optimum.

5.2.2 A solução proposta deverá proteger, no mínimo, os sistemas operacionais: Windows 7; Windows 8; Windows 8.1; Windows 10 e Windows 11. E as distribuições Linux CentOS 7.2 e posterior; Debian GNU/Linux 11.0 e posterior; Debian GNU/Linux 12.0 e posterior e Red Hat Enterprise Linux 7.2

e posterior; Ubuntu 22.04 LTS e posterior; Windows Small Business Server 2011; Windows MultiPoint Server 2011; Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022; Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022; Sistemas operacionais Linux de 32 e 64 bits.

5.2.3 Do módulo de gerenciamento avançado

5.2.3.1 A solução proposta deve suportar arquitetura cloud-native e on-premisse.

5.2.3.2 A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de: Amazon Web Services; Microsoft Azure; Google Cloud

5.2.3.3 A solução proposta deve incluir as seguintes opções de integração SIEM: HP (Microfoco) ArcSight; IBM QRadar; Splunk; Kaspersky KUMA.

5.2.3.4 A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

5.2.3.5 A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

5.2.3.6 A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

5.2.3.7 O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

5.2.3.8 A o modulo da solução on-premisse deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

5.2.3.9 A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

5.2.3.10 A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

5.2.3.11 A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

5.2.3.12 A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

5.2.3.13 O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

5.2.3.14 O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

- 5.2.3.14.1 Status do dispositivo
- 5.2.3.14.2 Tag
- 5.2.3.14.3 Diretório ativo
- 5.2.3.14.4 Proprietários de dispositivos
- 5.2.3.14.5 Hardware

5.2.3.15 A solução proposta deve suportar os seguintes canais de entrega de notificação:

- 5.2.3.15.1 E-mail
- 5.2.3.15.2 Registro de sistema
- 5.2.3.15.3 SMS

5.2.3.16 A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

- 5.2.3.16.1 Atributos de rede
- 5.2.3.16.2 Nome
- 5.2.3.16.3 Domínio e/ou Sufixo de Domínio
- 5.2.3.16.4 Endereço de IP

5.2.3.16.5 Endereço IP para servidor de gerenciamento

5.2.3.16.6 Localização no Active Directory

5.2.3.16.7 Unidade organizacional

5.2.3.16.8 Grupo

5.2.3.16.9 Sistema operacional

5.2.3.16.10 Número do pacote de serviço

5.2.3.16.11 Arquitetura Virtual

5.2.3.16.12 Registro de aplicativos

5.2.3.16.13 Nome da Aplicação

5.2.3.16.14 Versão do aplicativo

5.2.3.16.15 Fabricante

5.2.3.16.16 Tipo e versão

5.2.3.16.17 Arquitetura

5.2.3.17 A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

5.2.3.18 A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

5.2.3.19 As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

5.2.3.19.1 Dispositivos Desktop/Servidores

5.2.3.19.2. Dispositivos móveis

5.2.3.19.3 Dispositivos de rede

5.2.3.19.4 Dispositivos virtuais

5.2.3.19.5 Componentes OEM

5.2.3.19.6 Periféricos de computador

5.2.3.19.7 Dispositivos IoT conectados

5.2.3.19.8 Telefones VoIP

5.2.3.19.9 Repositórios de rede

5.2.3.20 A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

5.2.3.20.1 Nome da Aplicação

5.2.3.20.2 Caminho do aplicativo

5.2.3.20.3 Metadados do aplicativo

5.2.3.20.4 Aplicativo Certificado digital

5.2.3.20.5 Categorias de aplicativos predefinidas pelo fornecedor

5.2.3.20.6 SHA256 e MD5

5.2.3.21 A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

5.2.3.21.1 Bluetooth

5.2.3.21.2 Dispositivos móveis

5.2.3.21.3 Modems externos

5.2.3.21.4 CD/DVD

5.2.3.21.5 Câmeras e scanners

5.2.3.21.6 MTPs

5.2.3.21.7 E a transferência de dados para dispositivos móveis

5.2.3.22 A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

5.2.3.23 A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

5.2.3.24 A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

5.2.3.24.1 Estruturas de domínios e grupos de trabalho do Windows

5.2.3.24.2 Estruturas de grupos do Active Directory

5.2.3.24.3 Conteúdo de um arquivo de texto criado manualmente pelo administrador

5.2.3.25 A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

5.2.3.26 A solução proposta deve permitir realizar as seguintes ações para endpoints:

5.2.3.26.1 Verificação manual;

5.2.3.26.2 Verificação no acesso;

5.2.3.26.3 Verificação por demanda;

5.2.3.26.4 Verificação de arquivos compactados

5.2.3.26.5 Verificação de arquivos individuais, pastas e unidades;

5.2.3.26.6 Bloqueio e verificação de scripts

5.2.3.26.7 Proteção contra alteração de registros;

5.2.3.26.8 Proteção contra estouro de buffer;

5.2.3.26.9 Verificação em segundo plano/inativa

5.2.3.27 Verificação de unidade removível na conexão com o sistema;

5.2.3.28 A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.

5.2.3.29 O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.

5.2.3.30 A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.

5.2.3.31 A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.

5.2.3.32 A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.

5.2.3.33 A solução proposta deve suportar Windows Failover Cluster.

5.2.3.34 A solução proposta deve ter um recurso de clustering integrado.

5.2.3.35 A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.

5.2.3.36 A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

5.2.3.37 O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.

5.2.3.38 A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.

5.2.3.39 A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.

5.2.3.40 A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.

5.2.3.41 A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.

5.2.3.42 A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.

5.2.3.43 A solução proposta deverá possuir controles para download de DLL e drivers.

5.2.3.44 A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.

5.2.3.45 A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.

5.2.3.46 A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).

5.2.3.47 A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.

5.2.3.48 A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.

5.2.3.49 A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.

5.2.3.50 A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.

5.2.3.51 A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.

5.2.3.52 A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.

5.2.3.53 A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

5.2.3.54 A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.

5.2.3.55 A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.

5.2.3.56 A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.

5.2.3.57 A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .

5.2.3.58 A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.

5.2.3.59 A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

5.2.3.60 A solução proposta deve permitir ao administrador personalizar relatórios.

5.2.3.61 A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.

5.2.3.62 A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.

5.2.3.63 A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

5.2.3.64 A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

5.2.3.65 A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

5.2.3.66 A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

5.2.3.67 O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;

5.2.3.68 O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

5.2.3.69 A solução proposta deve suportar integração com solução APT.

5.2.3.70 A solução proposta deve suportar a integração com o serviço Managed Detection and Response.

5.2.3.71 A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

5.2.3.71.1 Linux

5.2.3.72 A solução proposta deverá suportar os seguintes servidores de banco de dados:

5.2.3.72.1 MySQL

5.2.3.72.2 MariaDB

5.2.3.72.3 PostgreSQL

5.2.3.74 A solução proposta deverá suportar as seguintes plataformas virtuais:

5.2.3.74.1 VMware vSphere 6.7 e 7.0

5.2.3.74.2 VMware Desktop 16 Pro e 17 Pro

5.2.3.74.3 Servidor Microsoft Hyper-V 2012 de 64 bits

5.2.3.74.4 Servidor Microsoft Hyper-V 2012 R2 de 64 bits

5.2.3.74.5 Microsoft Servidor Hyper -V 2016 de 64 bits

5.2.3.74.6 Servidor Microsoft Hyper-V 2019 de 64 bits

5.2.3.74.7 Servidor Microsoft Hyper-V 2022 de 64 bits

5.2.3.74.8 Citrix XenServer 7.1 e 8.x

5.2.3.74.9 Oracle VM VirtualBox 6.x e7.x

5.2.3.74.10 A solução proposta deve suportar criptografia em vários níveis:

5.2.3.74.11 Criptografia completa do disco – incluindo disco do sistema

5.2.3.74.12 Criptografia de arquivos e pastas

5.2.3.74.13 Criptografia de mídia removível

5.2.3.74.14 Gerenciamento de criptografia BitLocker e MacOS Filevault2

5.2.3.75 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:

5.2.3.75.1 A criptografia de arquivos em unidades de computador locais.

5.2.3.75.2 A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.

5.2.3.75.3 A criação de listas criptografadas de pastas em unidades de computador locais.

5.2.3.76 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:

5.2.3.76.1 Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.

5.2.3.76.2 Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

5.2.3.77 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:

5.2.3.77.1 A criptografia de todos os arquivos armazenados em unidades removíveis.

5.2.3.77.2 A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.

5.2.3.78 A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia

5.2.3.79 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.

5.2.3.80 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.

5.2.3.81 A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.

5.2.3.82 A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.

5.2.3.83 A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.

5.2.3.84 A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores /dispositivos criptografados.

5.2.3.85 A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.

5.2.3.86 A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.

5.2.3.87 A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

5.2.3.88 A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.

5.2.3.89 A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.

5.2.3.90 A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.

5.2.3.91 O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.

5.2.3.92 A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.

5.2.3.93 A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.

5.2.3.94 A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

5.2.3.94.1 Uso do Trusted Platform Module e configurações de senha.

5.2.3.94.2 Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.

5.2.3.95 Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).

5.2.3.96 A solução proposta deve suportar criptografia em Microsoft Surface Tablets.

5.2.3.97 A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:

5.2.3.97.1 Instalação remota de software de terceiros

5.2.3.97.2 Relatórios sobre software e hardware existentes

5.2.3.97.3 Monitoramento para instalação de software não autorizado

5.2.3.97.4 Remoção de software não autorizado

5.2.3.98 A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.

5.2.3.99 A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.

5.2.3.100 A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.

5.2.3.101 A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.

5.2.3.102 A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

5.2.3.103 A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.

5.2.3.104 O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.

5.2.3.105 A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança

5.2.3.106 A solução proposta deve permitir ao administrador aprovar atualizações.

5.2.3.107 A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.

5.2.3.108 A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.

5.2.3.109. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.

5.2.3.110 A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.

5.2.3.111 A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.

5.2.3.112 A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).

5.2.3.113 A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.

5.2.3.114 A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.

5.2.3.115 A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.

5.2.3.116 A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.

5.2.3.117 A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.

5.2.3.118 A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.

5.2.3.119 A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.

5.2.3.120 A solução proposta deve apoiar a implantação do sistema operacional.

5.2.3.121 A solução proposta deve suportar Wake-on LAN e UEFI.

5.2.3.122 A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.

5.2.3.123 A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.

5.2.3.124 A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.

5.2.3.125 A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.

5.2.3.126 A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

5.2.3.127 A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.

5.2.3.128 A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.

5.2.3.129 A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.

5.2.3.130 A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.

5.2.3.131 A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:

5.2.3.131.1 Inicie a instalação ao reiniciar ou desligar o computador.

5.2.3.131.2 Instale o gerador necessário todos os pré-requisitos do sistema.

5.2.3.131.3 Permitir a instalação de novas versões de aplicativos durante as atualizações.

5.2.3.131.4 Baixe atualizações para o dispositivo sem instalá-las.

5.2.3.132 A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.

5.2.3.133 A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.

5.2.3.134 O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

5.2.3.134.1 CEF;
5.2.3.134.2 LEEF;

5.2.3.135 A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

5.2.3.136 O relatório da solução proposta deve conter informações CVE.

5.2.3.137 A solução proposta deve suportar instalação de aplicações e software de terceiros;

5.2.4 Características Gerais

5.2.4.1 A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

5.2.4.1.1 Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

5.2.4.2 A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

5.2.4.3 A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).

5.2.4.4 A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.

5.2.4.5 A solução proposta deve suportar o subsistema Linux no Windows.

5.2.4.6 A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

5.2.4.6.1 Proteção contra ameaças sem arquivos (Fileless);

5.2.4.6.2 Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

5.2.4.7 A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;

5.2.4.8 A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.

5.2.4.9 A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.

5.2.4.10 A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.

5.2.4.11 A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.

5.2.4.12 A solução proposta deve fornecer análise comportamental baseada em machine learning.

5.2.4.13 A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.

5.2.4.14 A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

5.2.4.14.1 Controles de aplicativos,

5.2.4.14.2 Controle web e dispositivos

5.2.4.14.3 HIPS e Firewall

5.2.4.14.4 Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

5.2.4.14.5 Gerenciamento de criptografia de arquivos e discos;

5.2.4.14.6 Controle adaptativo para detecção de anomalias;

5.2.4.15 A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.

5.2.4.16 A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.

5.2.4.17 A solução proposta deve ter bancos de dados de reputação locais e globais.

5.2.4.18 A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.

5.2.4.19 A solução proposta deve incluir um módulo capaz, no mínimo, de:

5.2.4.19.1 Bloqueio de aplicativos com base em sua categorização.

5.2.4.19.2 Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.

5.2.4.19.3 A adição de sub-redes e a modificação de permissões de atividade.

5.2.4.20 A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.

5.2.4.21 A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

5.2.4.22 A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

5.2.4.23 A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:

5.2.4.23.1 Modo silencioso;

5.2.4.23.2 Discos rígidos e dispositivos removíveis;

5.2.4.23.3 De todos as contas de usuários do dispositivo.

5.2.4.24A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:

5.2.4.24.1 Exclusão imediata de dados;

5.2.4.24.2 Exclusão de dados adiada.

5.2.4.25 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:

5.2.4.25.1 Excluir usando os recursos do sistema operacional - os arquivos são excluídos;

5.2.4.25.2 Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

5.2.4.26 A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

5.2.4.27 A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

5.2.4.28 A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

5.2.4.29 A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

5.2.4.30 A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

5.2.4.31 A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

5.2.4.32 A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

5.2.4.33 A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

5.2.4.34 A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

5.2.4.35 A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

5.2.4.36 A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

5.2.4.37 A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

5.2.4.38 A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.

5.2.4.39 A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.

5.2.4.40 A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.

5.2.4.41 A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.

5.2.4.42 A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

5.2.4.43 A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.

5.2.4.44 A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.

5.2.4.45 A solução proposta deve ter categoria de detecção para bloquear banners de sites.

5.2.4.46 A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;

5.2.4.47 A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.

5.2.4.48 A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.

5.2.4.49 A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.

5.2.4.50 A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

5.2.4.51 A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.

5.2.4.52 A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.

5.2.4.53 A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.

5.2.4.54 O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.

5.2.4.55 O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.

5.2.4.56 A solução proposta deve suportar o controle de scripts executados em PowerShell.

5.2.4.57 A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

5.2.4.58 A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.

5.2.4.59 A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

5.2.4.60 A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

5.2.4.61 A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.

5.2.4.62 A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

5.2.4.63 A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

5.2.4.63.1 Filtro de anexos.

5.2.4.63.2 Verificação de mensagens de email ao receber, ler e enviar.

5.2.4.64 A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

5.2.4.65 A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

5.2.4.66 A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script etc.);

5.2.4.67 A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.

5.2.4.68 A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.

5.2.4.69 A solução proposta deve incluir suporte ao protocolo IPv6.

5.2.4.70 A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.

5.2.4.71 A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

5.2.4.72 Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

5.2.4.73 Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

5.2.4.74 A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

5.2.4.75 A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.

5.2.4.76 A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

5.2.4.77 A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

5.2.4.78 A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

5.2.4.79 A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

5.2.4.80 A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.

5.2.4.81 A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.

5.2.4.82 A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

5.2.4.83 A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

5.2.4.84 A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

5.2.4.85 A solução proposta deve suportar endereços IPv6.

5.2.4.86 A solução proposta deve suportar verificação em duas etapas (autenticação).

5.2.4.87 A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.

5.2.4.88 A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.

5.2.4.89 A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.

5.2.4.90 A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.

5.2.4.91 A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.

5.2.4.92 A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.

5.2.4.93 A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.

5.2.4.94 A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

5.2.4.95 A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.

5.2.4.96 A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.

5.2.4.97 A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

5.2.4.98 A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.

5.2.4.99 A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.

5.2.4.100 A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

5.2.4.101 A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.

5.2.4.102 A solução proposta deve ter a capacidade de excluir atualizações baixadas.

5.2.4.103 A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.

5.2.4.104 A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

5.2.4.105 A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

5.2.4.106 A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

5.2.4.107 Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

5.2.4.108 A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

5.2.4.109 A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.

5.2.4.110 A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

5.2.4.111 A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

> 5.2.4.111.1 Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

5.2.4.111.2 Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

5.2.4.112 A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

5.2.4.113 A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

5.2.5 **Do modulo de gerenciamento de dispositivos móveis**

5.2.5.1 O modulo deve ser integrado a console de gerenciamento;

5.2.5.2 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

5.2.5.2.1 Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

5.2.5.3 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

> 5.2.5.3.1 iOS 10–17 ou iPadOS 13–17

5.2.5.4 A solução proposta deve oferecer suporte a dispositivos Android Device Owner.

5.2.5.5 A solução proposta deve suportar dispositivos iOS supervisionados.

5.2.5.6 A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

5.2.5.7 A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

5.2.5.8 A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

5.2.5.9 A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).

5.2.5.10 A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.

5.2.5.11 A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

5.2.5.12 A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

5.2.5.13 A solução proposta deve ter recursos de conteinerização para dispositivos Android.

5.2.5.14 A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

5.2.5.14.1 Dados em contêineres

5.2.5.14.2 Contas de e-mail corporativo

5.2.5.14.3 Configurações para conexão à rede Wi-Fi corporativa e VPN

5.2.5.14.4 Nome do ponto de acesso (APN)

5.2.5.14.5 Perfil do Android for Work

5.2.5.14.6 Recipiente KNOX

5.2.5.14.7 Chave do gerenciador de licença KNOX

5.2.5.15 A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

5.2.5.15.1 Todos os perfis de configuração instalados

5.2.5.15.2 Todos os perfis de provisionamento

5.2.5.15.3 O perfil iOS MDM

5.2.5.16 Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

5.2.5.17 A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .

5.2.5.18 A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

5.2.5.18.1 Critérios de verificação do dispositivo;

5.2.5.18.2Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;

5.2.5.19 A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

5.2.5.20 A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

5.2.5.20.1 Cartões de memória e outras unidades removíveis

5.2.5.20.2 Câmera do dispositivo

5.2.5.20.3 Conexões Wi-Fi

5.2.5.20.4 Conexões Bluetooth

5.2.5.20.5 Porta de conexão infravermelha

5.2.5.20.6 Ativação do ponto de acesso Wi-Fi

5.2.5.20.7 Conexão de área de trabalho remota

5.2.5.20.8 Sincronização de área de trabalho

5.2.5.20.9 Definir configurações da caixa de correio do Exchange

5.2.5.20.10 Configurar caixa de e-mail em dispositivos iOS MDM

5.2.5.20.11 Configure contêineres Samsung KNOX.

5.2.5.20.12 Definir as configurações do perfil do Android for Work

5.2.5.20.13 Configurar e-mail/calendário/contatos

5.2.5.20.14 Defina as configurações de restrição de conteúdo de mídia.

5.2.5.20.15 Definir configurações de proxy no dispositivo móvel

5.2.5.20.16 Configurar certificados e SCEP

5.2.5.21 A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .

5.2.5.21.1 Portal de inscrição móvel KNOX

5.2.5.21.2 Pacotes de instalação pré-configurados independentes

5.2.5.22 A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.

5.2.5.23 A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.

5.2.5.24 A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

5.2.5.24.1 VMware AirWatch 9.3 ou posterior

5.2.5.24.2 MobileIron 10.0 ou posterior

5.2.5.24.3 IBM MaaS360 10.68 ou posterior

5.2.5.24.4 Microsoft Intune 1908 ou posterior

5.2.5.24.5 SOTI MobiControl 14.1.4 (1693) ou posterior

5.2.5.25 A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.

5.2.5.26 A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.

5.2.5.27 A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

5.2.5.28 A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.

5.2.5.29 A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.

5.2.5.30 A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.

5.2.5.31 A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.

5.2.5.32 A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.

5.2.5.33 A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.

5.2.5.34 A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.

5.2.5.35 A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.

5.2.5.36 A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.

5.2.5.37 A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.

5.2.5.38 A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;

5.2.5.39 A solução proposta deve proteger contra ameaças online em dispositivos iOS.

5.2.6 Do módulo de XDR

5.2.6.1 Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

5.2.6.2 Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

5.2.6.3 A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;

5.2.6.4 Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

5.2.6.5 Deve apresentar informações detalhadas contendo:

5.2.6.5.1 Usuário que executou a ação;

5.2.6.5.2 Informações acesso privilegiado;

5.2.6.5.6 A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

5.2.6.5.7 A solução proposta deve suportar integração com serviço de reputação em nuvem.

5.2.6.5.8 A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

5.2.6.5.9 O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).

5.2.6.5.10 Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;

5.2.6.5.11 A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

5.2.6.5.12 A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.

5.2.6.5.13 A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

5.2.6.5.14 A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

5.2.6.5.15 A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

5.2.6.5.16 A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

5.2.6.5.17 A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.

5.2.6.5.18 A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.

5.2.6.5.19 A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

5.2.6.5.20 A solução proposta deve permitir agregar os alertas com base nas seguintes informações:

5.2.6.5.20.1 Nome do dispositivo

5.2.6.5.20.2 Conta de usuário

5.2.6.5.20.3 Hash do arquivo

5.2.6.5.21 A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:

5.2.6.5.22 Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).

5.2.6.5.23 Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.

5.2.6.5.24 Informações gerais sobre a detecção, incluindo modo de detecção.

5.2.6.5.25 Alterações no registro associadas à detecção.

5.2.6.5.26 Histórico da presença de arquivos no dispositivo.

5.2.6.5.27 Ações de resposta executadas pela aplicação.

5.2.6.5.28 O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.

5.2.6.5.29 A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

5.2.6.5.29.1 Processo

5.2.6.5.29.2 Conexões de rede

5.2.6.5.29.3 Alterações no registro

5.2.6.5.29.4 Detalhes do download de objeto

5.2.6.5.30 A solução proposta deve fornecer orientação de resposta (resposta guiada).

5.2.6.5.31 A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente

5.2.6.5.32 A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:

5.2.6.5.32.1 Impedir a execução de objetos

5.2.6.5.32.2 Isolamento de host

5.2.6.5.32.3 Excluir objeto do host ou grupo de hosts

5.2.6.5.32.4 Encerrar um processo no dispositivo

5.2.6.5.32.5 Colocar um objeto em quarentena

5.2.6.5.32.6 Execute a verificação do sistema

5.2.6.5.32.7 Execução remota de programa/processo/comando

5.2.6.5.32.8 Iniciar a varredura IoC para um grupo de hosts.

5.2.6.5.32.9 Adicionar o usuário a um grupo de treinamento no módulo de conscientização

5.2.6.5.32.10 Bloquear o usuário no Active Directory

5.2.6.5.32.11 Resetar a senha do usuário no Active Directory

5.2.6.5.32.12 Adicionar o usuário em um grupo de segurança no Active Directory

5.2.6.5.32.13 Remover o usuário de um grupo de segurança no Active Directory

5.2.6.5.33 Deve possuir integração com solução de conscientização, sendo ela da mesma fabricante da solução de XDR

5.2.6.5.34 Deve possuir integração com o Active Directory para realizar respostas no mesmo

5.2.6.5.35 Deve possuir integração com o portal de inteligência do fabricante para fazer uma investigação detalhada do arquivo através do módulo de Sandbox em nuvem.

5.2.7 Do módulo de proteção para Microsoft Office 365

5.2.7.1 A solução deve ser entregue no modelo de “Software as a Service”, onde servidor e console administrativa são hospedados na nuvem.

5.2.7.2 Acesso a console administrativa via HTTPS.

5.2.7.3 A integração com o Office 365 deve ser realizada via API.

5.2.7.4 A autenticação da integração deve ser realizada via protocolo seguro OAuth 2.0.

5.2.7.5 A solução deve prover módulos de proteção para a suíte Microsoft Office 365 (Exchange Online, OneDrive, SharePoint e Teams).

5.2.7.6 A console deve prover painel de informações exibindo as informações principais da operação e do estado dos componentes de proteção.

5.2.7.7 Capacidade de geração de relatórios em no mínimo formato “.pdf”.

5.2.7.8 Capacidade de geração de relatório instantâneo;

5.2.7.9 Capacidade de agendamento automático de relatórios.

5.2.7.10 A solução deve verificar o tráfego de e-mails inbound e outbound.

5.2.7.11 Deve possuir quarentena para armazenar artefatos detectados como maliciosos.

5.2.7.12 A quarentena deve possuir no mínimo as seguintes opções:

5.2.7.13 Exibir detalhes do item;

5.2.7.14 Excluir item;

5.2.7.15 Liberar item;

5.2.7.16 Filtrar itens;

5.2.7.17 Salvar item em disco;

5.2.7.18 A gestão da solução deve ser realizada por usuário com perfil de administrador.

5.2.7.19 Deve ser possível atribuir perfil de administrador para um usuário na console de administração.

5.2.7.20 Deve ser capaz de detectar informação sensível em texto e imagens transmitidos e armazenados através da plataforma e alertar o administrador quanto ao risco de vazamento da informação.

5.2.7.21 Anti-malware

5.2.7.21.1 Deve proteger as caixas de correio contra vírus, worms, trojans, entre outras ameaças que podem ser enviadas via e-mail.

5.2.7.21.2 Análise das ameaças deve ser realizada por no mínimo as seguintes tecnologias:

5.2.7.21.3 Assinaturas;

5.2.7.21.4 Heurística;

5.2.7.21.5 Comportamento;

5.2.7.21.6 Consulta ao repositório de inteligência do fabricante.

5.2.7.21.7 Capacidade de detectar ataques conhecidos e desconhecidos.

5.2.7.21.8 Ao detectar um malware, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:

5.2.7.21.9 Excluir a mensagem e coloca-la em quarentena;

5.2.7.21.10 Excluir anexo infectado e colocá-lo em quarentena;

5.2.7.21.11 Colocar tag no assunto;

5.2.7.21.12 Substituir arquivo por mensagem personalizada;

5.2.7.21.13 Notificar ao administrador sobre novas ameaças encontradas

5.2.7.21.14 Notificar ao proprietário da caixa sobre mensagens excluídas.

5.2.7.21.15 Deve analisar arquivos nas seguintes aplicações:

5.2.7.21.16 Exchange Online

5.2.7.21.17 OneDrive

5.2.7.21.18 SharePoint

5.2.7.21.19 Teams

5.2.7.21.20 Ofercer proteção contra ataques mailsploit, ghost spoofing e injeções de código malicioso.

5.2.7.22 Anti-phishing

5.2.7.22.1Deve proteger as caixas de correio contra phishing e links maliciosos enviados em mensagens de e-mail, evitando assim infecção por malware, roubo de dados pessoas e acesso a sites fraudulentos.

5.2.7.22.2 Deve validar o conteúdo das mensagens para detectar phishing, utilizando as seguintes tecnologias:

5.2.7.22.3 SPF (Sender Policy Framework)

5.2.7.22.4 DKIM (Domain-based Message Authentication)

5.2.7.22.5 DMARC (Domain-based Message Authentication, Reporting and Conformance)

5.2.7.22.6 Consulta ao repositório de inteligência do fabricante.

5.2.7.22.7 Capacidade de detectar ataques conhecidos e desconhecidos.

5.2.7.22.8 Ao detectar um link de phishing, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:

5.2.7.22.9 Excluir a mensagem e coloca-la em quarentena;

5.2.7.22.10 Permitir;

5.2.7.22.10.1 Mover para pasta “Lixo eletrônico”;

5.2.7.22.10.2 Colocar tag no assunto;

5.2.7.22.10.3 Notificar ao administrador sobre novas mensagens encontradas.

5.2.7.22.10.4 Notificar ao proprietário da caixa sobre mensagens excluídas.

5.2.7.22.10.5 Permitir a criação de exclusões por e-mail completo ou máscara.

5.2.7.23 Anti-spam / Mass Mail

5.2.7.23.1 Deve proteger as caixas de correio contra e-mail não solicitados “SPAM” e e-mails enviados em massa.

5.2.7.23.2 A verificação deve ser realizada através dos seguintes métodos:

5.2.7.23.3 Verificação de cabeçalho, conteúdo, anexos e elementos de design;

5.2.7.23.4 Algoritmos linguísticos e heurísticos;

5.2.7.23.5 Consulta ao repositório de inteligência do fabricante;

5.2.7.23.6 Ao detectar um SPAM, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:

5.2.7.23.7 Permitir;

5.2.7.23.8 Mover para a pasta “Lixo eletrônico”;

5.2.7.23.9 Colocar tag no assunto;

5.2.7.23.10 Notificar ao administrador sobre novas ameaças encontradas

5.2.7.23.11 Notificar ao proprietário da caixa sobre mensagens excluídas.

5.2.7.23.12 Permitir a criação de exclusões por e-mail completo ou máscara.

5.2.8.24 Filtro de conteúdo

5.2.8.24.1 Deve possibilitar a filtragem de anexos em mensagens de e-mail.

5.2.8.24.2 Capacidade de detectar anexos pelos seguintes parâmetros:

5.2.8.24.3 Formato do arquivo;

5.2.8.24.4 Nome completo do arquivo;

5.2.8.24.5 Nome do arquivo com máscara;

5.2.8.24.6 Arquivos MS Office com macro;

5.2.8.24.7 Ao detectar um anexo que se encaixe em uma das regras, a solução deve possibilitar as seguintes ações:

5.2.8.24.8 Excluir mensagem e coloca-la em quarentena;

5.2.8.24.9 Excluir anexo e colocá-lo em quarentena;

5.2.8.24.10 Permitir

5.2.8.24.11 Colocar tag no assunto;

5.2.8.24.12 Substituir arquivo por mensagem personalizada;

5.2.8.24.13 Notificar ao administrador sobre novas ameaças encontradas

5.2.8.24.14 Notificar ao proprietário da caixa sobre mensagens excluídas.

5.2.8.24.15 Permitir a criação de exclusões por e-mail completo ou máscara.

5.2.8.25 Do módulo de treinamento de cibersegurança para administradores de TI

5.2.8.25.1 A plataforma de treinamento deve equipar os profissionais de TI com habilidades práticas para reconhecer um possível cenário de ataque em um incidente aparentemente benigno, competência para coletar dados de incidentes para a entrega de uma segurança de TI, criar uma paixão por procurar sinais de atividade maliciosa, consolidando o papel de todos os membros da equipe de TI como a primeira linha de defesa de segurança.

5.2.8.25.2 A plataforma de treinamento deve ser interativa, deve ter simulação de processos reais sem nenhum risco para o computador.

5.2.8.25.3 A plataforma de treinamento deve criar habilidades e conhecimentos, deve fornecer metodologia "Aprender fazendo".

5.2.8.25.4 A plataforma de treinamento deve ter um processo de aprendizado intuitivo, navegação conveniente e dicas.

5.2.8.25.5 A plataforma de treinamento deve abranger todos os principais tópicos e problemas de segurança de TI que a equipe geral de TI enfrenta em seu trabalho.

5.2.8.25.6 Os módulos da plataforma de treinamento on-line de segurança cibernética para TI devem conter os seguintes tópicos de treinamento:

5.2.8.25.6.1 Softwares Maliciosos

5.2.8.25.6.2 Programas e arquivos potencialmente indesejados (PuPs).

5.2.8.25.6.3 Noções básicas de investigação.

5.2.8.25.6.4 Segurança do servidor.

5.2.8.25.6.5 Segurança do Active Directory.

5.2.8.25.6.5 Phishing e inteligência de código aberto (OSINT).

5.2.8.26 Requisitos para certificados:

5.2.8.26.1 O usuário deve receber um certificado após a conclusão bem-sucedida do treinamento.

5.2.8.26.2 Os certificados devem ter o nome do cenário de treinamento, data de conclusão e nome do usuário.

5.2.8.26.3 O certificado deve ser apresentado em formato eletrônico na interface do usuário e estar disponível para download.

5.2.8.27 Requisitos para idiomas:

5.2.8.28 A interface da plataforma de treinamento, notificações automáticas por e-mail e todos os materiais de treinamento devem estar disponíveis nos seguintes idiomas:

5.2.8.28.1 Ingles.

5.2.8.28.2 Português.

5.2.8.29 Especificações técnicas da plataforma de treinamento:

5.2.8.30 A plataforma de treinamento deve suportar:

5.2.8.30.1 Windows - 10, 11.

5.2.8.30.2 Mac - Sierra, High Sierra, Mojave, Catalina.

5.2.8.30.3 Ubuntu 18.04.

5.2.8.30.4 Google Chrome - versão 80 ou superior.

5.2.8.30.5 Firefox - versão 70 e superior.

5.2.9 Do módulo de conscientização automatizada em cibersegurança para usuários finais

5.2.9.1 Deverá ter compatibilidade com os sistemas operacionais: Windows 10; Windows 11 e Linux.

5.2.9.2 Deverá ter compatibilidade com sistemas operacionais de dispositivos móveis: iOS 11 ou superiores;Android 5.x e superiores.

5.2.9.3 Deverá suportar os browsers: Microsoft Edge; Internet Explorer 11; Firefox; Google Chrome; Safari for MacOS; Safari(iOS); Google Chrome (Android).

5.2.9.4 Características da plataforma

5.2.9.4.1 A plataforma de treinamento deverá conter base de conhecimento com as principais dúvidas, dicas e guias de recomendações para o administrador da plataforma;

5.2.9.4.2 A plataforma deverá conter vídeos de demonstração de uso da solução;

5.2.9.5 A plataforma deverá conter uma base com possíveis mensagens/banner de alertas e segurança para compartilhamento dentro do programa de conscientização.

5.2.9.6 Durante a validade da licença, as atualizações da plataforma devem ser entregues sem ônus adicional;

5.2.9.7 Atualizações devem ser disponibilizadas para:

5.2.9.7.1 Atualização de conteúdo dos treinamentos;

5.2.9.7.2 Adição de novos conteúdos;

5.2.9.7.3 Novas funcionalidades para facilitar administração;

5.2.9.7.4 Novas funcionalidades para facilitar interação dos usuários;

5.2.9.7.5 Melhorias gerais do sistema e correção de bugs;

5.2.9.7.6 As atualizações na plataforma devem ser realizadas sem causar indisponibilidade ou afetar as funcionalidades;

5.2.9.7.7 O usuário deverá informar possíveis Phishing recebido, para isso a plataforma deve disponibilizar de funcionalidade ou plug-in para envio de notificação aos administradores;

5.2.9.7.8 O plano de atualização da plataforma deve:

5.2.9.7.8.1 Ser apresentado ao administrador da plataforma dias antes da sua execução;

5.2.9.7.8.2 Possibilitar ao administrador sugerir melhorias e votar estas melhorias durante a fase de discussão destas;

5.2.9.7.9 A interface da plataforma de treinamento, as notificações por e-mail e todo material de treinamento deverá ser disponibilizado minimamente nos idiomas Português, Inglês;

5.2.9.7.10 A plataforma deverá gerar automaticamente os seguintes relatórios de acompanhamento ao Administrador:

5.2.9.7.10.1 Relatório resumo com informações sobre o progresso dos usuários (enviado no mínimo semanalmente, com análise por categoria de desempenho, link para relatório completo e recomendações de alteração de categoria).

5.2.9.7.10.2 Relatório geral detalhado da empresa: lista de administradores, número de usuários, uso de licenças, categorias de desempenho, lista completa de usuários por grupo, datas de consentimento e conclusão, unidades expiradas, testes pendentes ou a repetir, certificados recebidos, exportação em XLSX e detalhamento de alunos em treinamento ou suspensos.

5.2.9.7.10.3 Relatório geral sobre grupos de treinamento, incluindo número de usuários, status de treinamento, usuários sem grupo, data de conclusão prevista e percentual concluído.

5.2.9.7.10.4 Relatório sobre o grupo de treinamento, com diagrama de meta e nível atual, e dados de atribuído/não iniciado/em treinamento/concluído/percentual concluído.

5.2.9.7.10.5 Relatório individual por usuário, incluindo atendimento aos treinamentos, dinâmica e atividade diária, histórico em formato de tabela (data, tipo de atividade, unidade, material, status, tempo gasto e total, recomendações, sessões agendadas, problemas de aprendizagem, nível de conhecimento e categoria de desempenho atual).

5.2.9.7.10.5.11 O usuário deverá receber e-mails semanais com relatórios de desempenho e de treinamento;

5.2.9.7.10.5.12 A plataforma deve definir no mínimo 5 (cinco) categorias de desempenho: "Antes do cronograma", "Indo bem", "Atrasado no cronograma", "Muito atrasado no cronograma", "Não terminará no prazo".

5.2.9.7.10.5.13 Cada usuário que está participando do treinamento deverá ser atribuído a uma dessas categorias de desempenho.

5.2.9.7.10.5.14 O acesso à plataforma de treinamento deve ser feito via internet, utilizando protocolos HTTPS e HTTP.

5.2.9.7.10.5.15 O administrador da plataforma de treinamento deve ser capaz de gerenciar o processo de treinamento de todos os usuários;

5.2.9.7.10.5.16 A plataforma de treinamento deve permitir que o administrador crie e remova empresas;

5.2.9.7.10.5.17 A plataforma de treinamento deve ser capaz de atribuir uma empresa específica a um administrador e restringir o acesso desse administrador a outras empresas;

5.2.9.7.10.5.18 A plataforma de treinamento deve ser capaz de atribuir privilégios diferentes para 4 funções de administrador. Cada administrador pode visualizar e/ou gerenciar apenas nas empresas às quais está atribuído;

5.2.9.7.10.5.19 O administrador deve ser capaz de configurar todos os parâmetros da empresa e parâmetros de perfil do usuário, inserir dados do usuário, definir um conjunto de grupos de treinamento em cada empresa, alterar o programa de treinamento no grupo de treinamento, distribuir usuários entre os grupos de treinamento, atribuir e controlar o treinamento do usuário.

5.2.9.7.10.5.20 A plataforma deverá enviar notificações automáticas aos usuários, nos requisitos abaixo:

5.2.9.7.10.5.20.1 Os funcionários de um grupo que iniciou o treinamento deverão receber um e-mail com convite para seguir um link exclusivo, gerado pela plataforma usando o nome de domínio especificado pelo Administrador nas configurações da empresa.

5.2.9.7.10.5.20.2 O usuário deve receber automaticamente relatórios semanais de treinamento por e-mail. Tais relatórios deverão incluir a categoria de desempenho atual do usuário e recomendações sobre as unidades de treinamento atribuídas.

5.2.9.7.10.5.20.3 O administrador deve ser capaz de configurar parâmetro de checagem de domínio para não enviar informações de inicio de campanhas e garantir que soluções de proteção contra phishing não bloqueie as campanhas executadas pela plataforma.

5.2.10.6 Requisitos para definir os parâmetros de uma empresa

5.2.10.6.1 O administrador deve ser capaz de definir os seguintes parâmetros de uma empresa:

5.2.10.6.1.1 Nome da empresa;

5.2.10.6.1.2 Nome de domínio de quarto nível do nome de domínio do site onde os usuários dessa empresa são treinados;

5.2.10.6.1.3 Idioma padrão (em particular, o idioma usado no primeiro convite enviado ao usuário);

5.2.10.6.14 Nome e endereço de correspondência do funcionário que desempenha as funções de suporte técnico aos usuários;

5.2.10.6.1.5 Campos (ou atributos) do perfil do usuário nessa empresa. O administrador deve ser capaz de adicionar atributos personalizados ou excluir atributos que foram adicionados anteriormente;

5.2.10.6.1.6 Regras para alocar usuários automaticamente em grupos de treinamento;

5.2.10.6.1.7 Saudações nas mensagens que os usuários recebem da plataforma;

5.2.10.6.1.8 Nome de usuário mostrado e certificados emitidos quando as unidades de treinamento são concluídas.

5.2.10.7 Requisitos para usar licenças de usuário

5.2.10.7.1 O administrador deve ser capaz de adicionar ou excluir licenças.

5.2.10.7.2 A plataforma não deve estabelecer uma conexão direta entre um usuário específico e uma licença específica.

5.2.10.7.3 A plataforma deve controlar os seguintes parâmetros relacionados à Licença:

5.2.10.7.3.1 O número de usuários na fase ativa de treinamento;

5.2.10.7.3.2 O número de licenças disponíveis.

5.2.10.7.4 Quando o administrador atribui treinamento a um usuário, o número de licenças usadas deve aumentar;

5.2.10.7.5 Quando o administrador interromper ou suspender o treinamento de um usuário, o número total de licenças usadas deve diminuir.

5.2.10.8 Requisitos para gerenciamento de treinamento

5.2.10.8.1 O administrador deve ser capaz de atribuir um programa de treinamento, dependendo da posição do funcionário e do grau de risco de segurança cibernética (conforme definido pela organização).

5.2.10.8.2 A plataforma deve executar automaticamente as seguintes etapas:

5.2.10.8.2.1 Criar horários de aula para grupos e cada usuário, com base no nível de destino selecionado do grupo;

5.2.10.8.2.2 Enviar notificações por e-mail automaticamente aos usuários;

5.2.10.8.2.3 Enviar automaticamente lembretes aos usuários informando que eles podem prosseguir para aproxima tarefa em um determinado estágio;

5.2.10.8.2.4 Criar e ajustar um cronograma de treinamento individual para cada funcionário;

5.2.10.8.2.5 Atribuir todos os materiais de treinamento ao usuário;

5.2.10.8.2.6 Acompanhar o progresso do treinamento de cada usuário;

5.2.10.8.2.7 Fornecer relatórios de desempenho semanais aos usuários;

5.2.10.8.2.8 Enviar e-mails aos usuários com recomendações personalizadas, para que possam concluir o curso no prazo e com sucesso;

5.2.10.8.2.9 Enviar e-mails ao administrador com relatórios semanais, incluindo recomendações sobre como motivar um usuário para a comunicação fora da plataforma de treinamento.

5.2.10.9 Requisitos para gerenciamento de usuários

5.2.10.9.1 A plataforma deve permitir que o Administrador execute as seguintes tarefas:

5.2.10.9.1.1 Adicionar, editar, arquivar, restaurar, excluir um usuário ou grupo de usuários;

5.2.10.9.1.2 Adicionar usuários à plataforma importando uma lista de usuários de um arquivo XSLX.

5.2.10.9.2.1 O arquivo modelo deve estar disponível no site da plataforma;

5.2.10.9.1.3 Criar grupos e transferir usuários entre estes;

5.2.10.9.2 A plataforma deve ser capaz de se integrar com o Microsoft Active Directory e com outros sistemas via OpenAPI para sincronizar listas de usuários.

5.2.10 Requisitos para gerenciamento de grupos

5.2.10.1 O programa de treinamento deve permitir que o Administrador use os grupos de treinamento que existem por padrão ou crie um número ilimitado de novos grupos de treinamento;

5.2.10.2 O programa de treinamento deve permitir que o Administrador altere os parâmetros de treinamento para grupos, como o nome do grupo, o conjunto de tópicos, o nível de destino de cada tópico (definição de quantas sessões o usuário deve realizar neste tópico), a intensidade (define quantos minutos por semana o usuário é recomendado utilizar na plataforma).

5.2.10..2.1 O administrador atribui o nível de treinamento alvo dependendo do risco que cada usuário específico no grupo específico pode representar para a empresa. Quanto maior o risco, maior o nível de destino precisa ser.

5.2.10.2.2 Os níveis (“Iniciante”,”Elementar”,”Intermediário”) são distribuídos respectivamente de acordo com o nível de risco – de baixo a alto.

5.2.10.3 Por padrão, a plataforma deve ter três grupos correspondentes aos três diferentes níveis de treinamento:

5.2.10.3.1 Iniciante: Para funcionários com acesso limitado aos sistemas corporativos de TI;

5.2.10.3.2 Elementar: Para funcionários com acesso total à rede corporativa, mas sem acesso a informações especialmente confidenciais.

5.2.10.3.3 Intermediário: Para funcionários que têm acesso a informações confidencias e dados pessoais, bem como acesso de administrador em seus computadores.

5.2.10.4 A plataforma de treinamento deve permitir que o administrador crie regras para mover usuários automaticamente para grupos de treinamentos quando são adicionados à plataforma de treinamento.

5.2.10.5 Para cada grupo de treinamento, o cronograma de treinamento deve ser calculado automaticamente de acordo com a intensidade do treinamento, a data de início do treinamento e nível alvo para cada um dos tópicos selecionados.

5.2.10.6 O cronograma de treinamento deve ser alterado de acordo com a intensidade de treinamento selecionada pelo Administrador da plataforma.

5.2.10.7 A plataforma de treinamento deve ser capaz de iniciar e interromper o treinamento de um grupo de usuários ou de um usuário específico.

5.2.10.8 A plataforma de treinamento deve ser capaz de iniciar o treinamento para todos os usuários de um grupo específico.

5.2.10.9 A plataforma de treinamento deve ser capaz de adicionar um usuários a um grupo de treinamento.

5.2.11 Requisitos de metodologia de treinamento

5.2.11.1 O programa de treinamento deve ser elaborado de acordo com os seguintes princípios:

5.2.11.1.1 Os materiais de formação devem constituir um programa de formação, ou seja, os conteúdos e a quantidade de conhecimentos e competências em segurança cibernética necessários à aprendizagem obrigatória, bem como a sua distribuição por tópico, seção e nível de dificuldade;

5.2.11.1.2 Ao passar dos tópicos, o material de aprendizagem aumenta o nível de dificuldade em relação a apresentação de técnicas cibercriminosas mais avançadas e das contra-medidas relacionadas;

5.2.11.1.3 Cada tópico deve ser apresentado pelo mesmo conjunto de materiais de treinamento;

5.2.11.1.4 A estrutura da aula deve ser a mesma para todos os tópicos;

5.2.12 Requisitos para o conteúdo dos materiais de treinamento

5.2.12.1 O programa de treinamento da plataforma deve incluir, no mínimo, os seguintes tópicos:

5.2.12.1.1 Senhas e contas;

5.2.12.1.2 Segurança de E-mail;

5.2.12.1.3 Navegação na Web;

5.2.12.1.4 Redes sociais e serviços de mensageria;

5.2.12.1.5 Segurança do PC:

5.2.12.1.6 Dispositivos móveis;

5.2.12.1.7 Informação Confidencial;

5.2.12.1.8 LGPD;

5.2.12.1.9 Segurança de cartões de banco;

5.2.12.1.10 PCI DSS;

5.2.12.1.11 Infraestrutura industrial;

5.2.12.2 O programa de treinamento deve incluir lições com temas atuais que possam desenvolver as habilidades dos usuários nas seguintes áreas de segurança cibernética:

5.2.12.2.1 Phishing;

5.2.12.2.2 Links maliciosos;

5.2.12.2.3 Ransomware;

5.2.12.2.4 Arquivos perigosos;

5.2.12.2.5 Aplicações maliciosas;

5.2.12.2.6 Engenharia social;

5.2.13 Requisitos para o programa de treinamento

5.2.13.1 Cada tópico deve ser dividido em vários níveis dedicados à prática de um grupo específico de habilidades no campo da segurança cibernética.

5.2.13.2 Cada nível do programa deve corresponder a ameaças com vários graus de gravidade, desde ataques básicos e em larga escala até proteção contra-ataques complexos e direcionados.

5.2.13.3 Cada tópico deve incluir aulas (exercícios), material para reforço (e-mail), teste de conhecimento e simulação de um ataque de phishing.

5.2.13.4 Para concluir um tópico com sucesso, o usuário deve fazer o teste de conhecimento relacionado.

5.2.13.5 A transição para o próximo nível deve ser possível depois que todos os tópicos anteriores no nível apropriado foram realizados e o teste de conhecimento relacionado aprovado com sucesso.

5.2.13.6 O usuário deve ter a opção de passar em um tópico com antecedência, realizando com sucesso o teste de conhecimento antes de aprender os materiais do tópico.

5.2.14 Requisitos para materiais de treinamento

5.2.14.1 A estrutura de aulas (incluindo exercícios) para cada tópico deve ser a mesma em todos os tópicos e deve seguir a sequência lógica abaixo:

5.2.14.1.1 Um conjunto de ações a serem realizadas;

5.2.14.1.2 Por que um usuário deve realizar essas ações;

5.2.14.1.3 As consequências potenciais de ações incorretas;

5.2.14.1.4 Os sinais de perigo que um usuário deve identificar;

5.2.14.1.5 As ações que um usuário deve realizar ao detectar sinais de perigo;

5.2.14.1.6 O que fazer se as dúvidas permanecerem.

5.2.14.2 Os seguintes tipos de materiais de treinamento devem ser apresentados:

5.2.14.2.1 Aulas, incluindo parte teórica e exercícios práticos com feedback;

5.2.14.2.2 Testes de conhecimento;

5.2.14.2.3 Simulações de ataque de phishing;

5.2.14.2.4 Exercícios de reforço.

5.2.14.3 As aulas devem incluir:

5.2.14.3.1 Slides a serem estudados;

5.2.14.3.1.1 Devem conter:

5.2.14.3.1.1.1 Informações textuais e gráficas;

5.2.14.3.1.1.2 Botões para avançar e retornar aos slides;

5.2.14.3.1.1.3 Questões para autoavaliação;

5.2.14.4 Os exercícios de reforço devem consistir em coleção de conselhos ou recomendações para exercícios anteriores, bem como exemplos reais de consequências do não cumprimento das regras de segurança cibernética.

5.2.14.5 O teste deve consistir em questões às quais o usuário deve dar uma resposta ou múltipla escolha de opções.

5.2.14.6 Os resultados do teste devem indicar a aprovação ou não.

5.2.14.7 Deve ser possível definir um valor mínimo de acertos para êxito no teste.

5.2.14.8 Quando o teste for concluído, o usuário poderá dar feedback para cada questão, independentemente de ter respondido corretamente.

5.2.14.9 Os ataques simulados de phishing devem permitir que a reação do usuário à ameaça cibernética seja verificada;

5.2.14.10 Os materiais de treinamento devem ser adaptados para usuários que suas contas pessoais em um navegador de dispositivo móvel.

5.2.15 Requisitos para funcionalidade de simulação de ataques phishing

5.2.15.1 A plataforma de treinamento deve abranger duas opções de atribuição de ataques simulados de phishing:

5.2.15.1.1 Integrado ao caminho de aprendizagem automatizado para dominar especificamente o conjunto de habilidades criadas nas lições anteriores da unidade.

5.2.15.1.2 Possibilidade de criar uma companha de phishing separada para um grupo específico de usuário não relacionados a nenhuma atividade de treinamento;

5.2.15.1.3 Um ataque de phishing simulado deve ser semelhante a uma mensagem real na forma de um texto com layout, imagens (opcional) e um link. Quando clicado,o link deve redirecionar o usuário para uma página simulada especial;

5.2.15.1.4 A página simulada para qual o usuário foi redirecionado no ataque simulado de phishing deve conter uma explicação sobre o motivo pelo qual o usuário foi parar naquele site, uma descrição do email que o usuário receber, bem como recomendações sobre o reconhecimento de e-mails de phishing.

5.2.15.1.5 A plataforma deve conter pelo menos trinta modelos de phishing diferentes que são enviados aos usuários durante o treinamento;

5.2.15.1.6 A campanha deve possibilitar ser agendada ou ser enviada imediatamente;

5.2.15.1.7 O usuário deve receber um ataque simulado de phishing em até 4 dias da conclusão com sucesso, dos testes de conhecimento do tópico de treinamento relacionado;

5.2.15.1.8 Quando configurada separada do programa de aprendizagem, a campanha de phishing deverá incluir vários modelos para o grupo de pessoas para envio aleatório de um determinado modelo para cada funcionário.

5.2.15.1.9 O usuário deverá ser considerado como aprovado no ataque de phishing simulado se ele (a) não clicar no link do email e não for direcionado para a página simulada.

5.2.15.1.10 Caso o usuário falhe na simulação, esta deverá acontecer novamente dentro do prazo de 4 (quatro) dias (caso o phishing simulado esteja integrado no caminho de aprendizagem automatizado).

5.2.16 Requisitos para o cronograma de treinamento

5.2.16.1 O cronograma de treinamento deve ser baseado nos seguintes intervalos de tempo:

5.2.16.1.1 O material de reforço deve estar disponível após realização dos exercícios teóricos e práticos;

5.2.16.1.2 O teste de conhecimento deve estar disponível após o material de reforço;

5.2.16.1.3 A simulação de ataque de phishing deve ser enviada ao usuário após conclusão bem-sucedida dos testes de conhecimento;

5.2.16.2 Os materiais de treinamento deverão ser disponibilizados ao usuário conforme prazo estipulado;

5.2.16.3 O cronograma de treinamento deve se readequar de forma automática à velocidades diferentes dos usuários;

5.2.16.4 O usuário deverá ser aprovado no teste para um tópico específico antes de passar para o próximo tópico;

5.2.16.5 O usuário deverá ser capaz de refazer o teste reprovado após conclusão do treinamento;

5.2.16.6 No caso do usuário falhar no ataque de phishing simulado, este deve ser reenviado automaticamente em até 4 dias ao usuário;

5.2.16.7 O cronograma de treinamento do usuário deve ser baseado na intensidade de treinamento, não restringindo o usuário de fazer as aulas teóricos em seu ritmo. Conforme a intensidade aumentar, as quantidades de materiais teóricos atribuídos ao usuário também aumentarão.

5.2.16.8 A plataforma deve calcular automaticamente a programação do usuário com base no programa de treinamento do grupo.

5.2.17 Requisitos para a conta pessoal do usuário da plataforma

5.2.17.1 Cada usuário deve ter uma conta pessoal única onde tarefas, histórico de treinamento, informações sobre desempenho e progresso estarão disponíveis;

5.2.17.2 A conta pessoal deve ser uma página da web acessível ao usuário através de um link exclusivo que o usuário recebe por meio de notificações por email;

5.2.17.3 O histórico de treinamento deve incluir uma lista de todas as tarefas concluídas e seus respectivos resultados;

5.2.17.4 O usuário deverá ser capaz de retornar ao material preenchido anteriormente para repetir o treinamento;

5.2.17.5 Na conta pessoal do usuário, deverão haver informações sobre andamento e estatísticas sobre os materiais abordados;

5.2.17.6 As estatísticas de treinamento devem ser visíveis par ao usuário:

5.2.17.6.1 Informações sobre o nível sobre a habilidade alvo do usuário;

5.2.17.6.2 Porcentagem de habilidade adquiridas até o momento do número total de habilidades para um determinado nível alvo;

5.2.17.6.3 Data planejada de conclusão do treinamento;

5.2.17.6.4 Data prevista de conclusão;

5.2.17.7 A data prevista de conclusão do treinamento do usuário deve ser calculada de acordo com a programação do grupo do qual o usuário faz parte;

5.2.17.8 A data de conclusão da unidade no plano de treinamento do usuário deve ser determinada com base na data planejada do teste e o tempo que o usuário requer para fazer o teste;

5.2.17.8.9 Na página de treinamento do usuário deverá haver conselhos e recomendações que ajudarão o usuário a concluir o treinamento no prazo;

5.2.17.8.10 A conta pessoal do usuário deve ser totalmente adaptada para que possa ser usada em dispositivos móveis.

5.2.18 Requisitos para certificados

5.2.18.1 O usuário deve receber um certificado após a conclusão bem-sucedida de cada tópico realizado;

5.2.18.2 O tópico deve ser considerado concluído com êxito quando o usuário tiver concluído com êxito o teste e for aprovado na simulação de ataque de phishing;

5.2.18.3 O certificado deve ser apresentado em formato eletrônico na interface do usuário e estar disponível para download;

5.2.18.4 O administrador deve ter a possibilidade de escolher como representar o nome do funcionário e outros campos personalizados no certificado.

5.2.19 Requisitos para customização

5.2.19.1 Logo da instituição:

5.2.19.1.1 O Administrador deve ser capaz de adicionar o logotipo da empresa na conta da plataforma;

5.2.19.2 Saudações ao aluno:

5.2.19.2.1 O administrador deve ser capaz de personalizar a saudação do funcionário em notificações por e-mail enviadas aos alunos pela plataforma – como convites, lembretes e recomendações.

5.2.19.2.2 A possibilidade deve dar a capacidade de fazer essas saudações mais adequadas às especificidades do país e/ou cultura de diferentes clientes.

5.2.19.2.3 O administrador deve ser capaz de adicionar qualquer texto ou usar marcas para criar o texto necessário.

5.2.19.2.4 As tags devem incluir o nome completo do usuário, saudação curta e todos os campos personalizados criados para esta empresa.

5.2.19.3 Certificados dos alunos:

5.2.19.3.1 O administrador deve ser capaz de personalizar a aparência do nome do aluno no ceritficado;

5.2.19.3.2 O administrador deve ser capaz de adicionar qualquer texto ou usar marcas para criar o texto necessário;

5.2.19.3.2.1 As tags devem incluir o nome completo do usuário, saudação curta e todos os campos personalizados criados para esta empresa.

5.2.19.4 Personalização do programa educacional:

5.2.19.4.1 Este recurso deve dar ao administrador a possibilidade de gerenciar o processo de aprendizagem para a empresa:

5.2.19.4.1.1 Desativar/ativar os primeiros testes de teste que permitem ao usuário pular a teoria;

5.2.19.4.1.2 Desativar/ativar a simulação de phishing que é incluída automaticamente no caminho de aprendizagem;

5.2.19.4.1.3 Escolher o nível alvo e os tópicos a serem atribuídos ao grupo de usuários.

5.2.19.5 Personalização do caminho de aprendizagem:

5.2.19.5.1 Para cada grupo de treinamento, o administrador deve ser capaz de selecionar:

5.2.19.5.1.1 Tópicos que os alunos neste grupo precisam aprender (e pular aqueles que você não deseja treinar agora).

5.2.19.5.1.2 Nível alvo desejado para que os alunos atinjam em cada tópico específico.

5.2.19.6 Personalização de ataques de phishing simulados:

5.2.19.6.1 Possibilidade de personalizar template de phishing com assunto, textos e fotos e salvar na biblioteca;

5.2.19.6.2 Variedade de domínios de phishing e endereços de e-mail de remetentes para personalização.

5.2.19.6.3 O administrador poderá criar campanhas de Phishing sem a necessidade de consentimentos dos usuários, Campanhas de Phishing “Cegos”

5.2.19.6.4 A plataforma deverá permitir o uso de QR Codes em phishing customizados,

5.2.19.6.5 A plataforma deverá permitir o uso de anexos aos e-mail de phishing customizados com o seguintes formatos: ZIP e PDF.

5.2.20 Do modulo de Sandbox em nuvem

5.2.20.1 Deve possuir uma solução que permita a execução de arquivos em ambientes isolados

5.2.20.2 A solução deve possuir os seguintes status para cada análise feita:

5.2.20.2.1 Limpo

5.2.20.2.2 Malware

5.2.20.2.3 Adware ou outros

5.2.20.2.4 Não confiável

5.2.20.2.5 Não categorizado

5.2.20.3 A solução deve suportar análise de objetos compactados (arquivos compactados e arquivados)

5.2.20.4 A solução deve manter os resultados do histórico de análise de arquivos por pelo menos 180 dias por padrão

5.2.20.5 A solução deve suportar todos os tipos de arquivos (executáveis, outros formatos, ou seja, PDF, MS office, scripts java, arquivos de certificado, etc.)

5.2.20.6 A solução deve suportar a exportação de resultados de análise de arquivos para vários formatos, tais como:

5.2.20.6.1 STIX;

5.2.20.6.2 CSV;

5.2.20.6.3 JSON;

5.2.20.6.4 PCAP;

5.2.20.6.5 DEBUG Report;

5.2.20.7 A solução deverá suportar configurações personalizadas para análise de artefatos, deve conter no mínimo:

5.2.20.7.1 Ambiente de execução;

5.2.20.7.2 Tempo de execução do artefato;

5.2.20.7.3 Tipos de conexão;

5.2.20.7.4 Senha dos arquivos internos;

5.2.20.7.5 Comandos e parâmetros;

5.2.20.7.6 Clique em links;

5.2.20.8 A solução deverá ter sandbox com informações de sumario executivo, contendo no mínimo:

5.2.20.8.1 Arquivos detectados dentro da amostra;

5.2.20.8.2 Atividades maliciosas;

5.2.20.8.3 Atividades de rede;

5.2.20.9 A solução deverá ter sandbox com informações técnicas, contendo no mínimo:

5.2.20.9.1 Mapa de execução do artefato contendo, detalhes técnicos e técnica utilizada mapeada pelo MITRE ATT&CK;

5.2.20.9.2 Tabela com as Técnicas e tácticas mapeadas a partir do MITRE do artefato analisado.

5.2.20.9.3 Screentshot das telas e comportamentos do artefato.

5.3 Características adicionais para a Solução de Antivírus item 2

5.3.1 A solução ofertada para o item 2, deverá possuir todas as características listadas no item 5.2 e adicionalmente os requisitos listados a seguir:

5.3.2 Do monitoramento, identificação e investigação dos eventos de segurança cibernética

5.3.3 O serviço de monitoramento deverá utilizar informações extraídas de registros gerados pelos sistemas monitorados.

5.3.4 Deverá ser instalado agentes específicos nos servidores e desktops, objetivando coletar informações mais detalhadas para o serviço de monitoramento, desde que seja plenamente compatível com o sistema onde será instalado e não afete o desempenho dos serviços.

5.3.5 A análise das informações correlacionadas deve ser realizada com auxílio de bases globais de inteligência cibernética em conjunto com a expertise dos profissionais do fabricante, com vistas a reduzir ao máximo os falsos positivos.

5.3.6 É obrigatório que a comunicação entre equipamentos e soluções do fabricante instalados nos dispositivos e qualquer infraestrutura onde esses dados sejam processados ocorra de forma segura, utilizando algoritmos criptográficos para preservar o sigilo das informações.

5.3.7 Deverá ser feita a investigação e a classificação dos eventos monitorados, aplicando os principais frameworks de gestão de incidentes de segurança cibernética bem como boas práticas de mercado na detecção e triagem dos eventos de segurança, objetivando minimizar a presença de falsos positivos na abertura de incidentes de segurança.

5.3.8 O serviço de monitoramento deverá ser capaz de coletar e realizar a correlação de eventos dos sistemas e ativos monitorados, permitindo uma visão mais abrangente do alcance das ações maliciosas, bem como de possível movimentação lateral do atacante dentro da rede.

5.3.9 Deverá monitorar e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média e identificando comportamentos anômalos, visando antecipar a identificação de incidentes de segurança.

5.3.10 A solução deverá prover inteligência de proteção contra ataques cibernéticos a nível global, sendo responsável por pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança monitorados.

5.3.11 O fabricante deverá utilizar solução para registro de incidente de segurança, acessível pela equipe técnica da Contratante, para indicar ações de contenção, comunicar à equipe da Contratante sobre o andamento do tratamento dos incidentes.

5.3.12 Compatibilidade:

5.3.12.1 É suportada por qualquer um dos seguintes navegadores:

5.3.12.1.1 Apple Safari versões mais recentes

5.3.12.1.2 Google Chrome versões mais recentes

5.3.12.1.3 Microsoft Edge

5.3.12.1.4 Mozilla Firefox versões mais recentes

5.3.13 Requisitos de rede:

5.3.13.1 Em condições médias de carga: um canal full-duplex com largura de banda de pelo menos 1,7 Kbps para cada ativo.

5.3.13.2 Em condições de carga máxima: um canal full-duplex com largura de banda de pelo menos 2,7 Kbps para cada ativo.

5.3.14 Compatibilidade de sensor de endpoint

5.3.14.1 O agente de endpoint deve ser compatível com os seguintes sistemas operacionais, para no mínimo a coleta e envio dos dados /telemetria ao SOC do fabricante:

5.3.14.1.1 Microsoft Windows 7 e superiores;

5.3.14.1.2 macOS 10.14-11;

5.3.14.1.3 CentOS 7.2 ou superior;

5.3.14.1.4 Debian GNU / Linux 9.4 ou superior;

5.3.14.1.5 Linux Mint 19 ou superior;

5.3.14.1.6 Oracle Linux 7.3 ou superior;

5.3.14.1.7 Red Hat Enterprise Linux 7.2 ou superior;

5.3.14.1.8 SUSE Linux Enterprise Server 12 SP5 ou superior;

5.3.14.1.9 Ubuntu 18.04 LTS ou superior.

5.3.15 Capacidades técnicas

5.3.15.1 Deve possuir console web própria do serviço, além de integração nativa com a console do “software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets”

5.3.15.2 A console deve possuir dashboards com as informações principais, apresentando no mínimo:

5.3.15.3 Número de incidentes e status

5.3.15.4 Quantidade de dispositivos monitorados

5.3.15.5 Deve possuir mecanismo de notificações, com no mínimo as seguintes opções:

5.3.15.5.1 E-mail

5.3.15.5.2 Telegram

5.3.15.6 Deve permitir o envio de relatórios.

5.3.15.7 O agente deve enviar a telemetria em tempo real para o SoC do fabricante;

5.3.15.8 O serviço deve compreender monitoramento dos dados enviados e alertas gerados em um regime 24x7x365.

5.3.15.9 O envio e armazenamento da telemetria, devem respeitar as principais legislações de proteção de dados, como GDPR e LGPD.

5.3.15.10 O SoC do fabricante deve possuir datacenters em pelo menos duas localidades em diferentes países.

5.3.15.11 O SoC do fabricante deve possuir equipes de analistas em pelo menos 3 regiões (países) incluindo Brasil.

5.3.15.12 Os dados coletados devem passar por no mínimo:

5.3.15.12.1 Modelos de Machine Learning/Inteligência Artificial;

5.3.15.12.2 Análise humana;

5.3.15.12.3 Correlação com IoA’s (indicadore de ataque);

5.3.15.12.4 Emulação em sandbox (quando necessário);

5.3.15.13 Após análise, informações sobre atividades potencialmente maliciosas, devem ser apresentadas no portal como “Incidentes”

5.3.15.14 O Incidente deve possuir no mínimo as seguintes informações:

5.3.15.14.1 Resumo

5.3.15.14.2 Prioridade (Baixa, Média e Alta)

5.3.15.14.3 Recomendação

5.3.15.14.4 Data de criação e data de atualização

5.3.15.14.5 Correlacionamento com táticas/técnicas do Framewok MITRE ATT&CK

5.3.15.14.6 Dispositivos afetados

5.3.15.14.7 IoC’s de host e de rede

5.3.15.14.8 Descrição completa em linha do tempo

5.3.15.15 O incidente pode receber ações de resposta recomendada disparadas pela equipe de SoC, compreendendo no mínimo as seguintes ações:

5.3.15.15.1 Transferir arquivo para o SoC;

5.3.15.15.2 Isolar um dispositivo;

5.3.15.15.3 Desabilitar isolamento de dispositivo;

5.3.15.15.4 Deletar chave de registro;

5.3.15.15.5 Dump de memória;

5.3.15.16 As ações devem ser aprovadas no portal por profissional da contratante, com a opção de habilitar aprovação automática.

5.3.15.17 Deve possuir console mult-tenant com a possibilidade de separar ativos.

5.3.15.18 Deve possuir campos para o mult-tenant para melhor visualização:

5.3.15.18.1 Name;

5.3.15.18.2 Status;

5.3.15.18.3 Descrição;

5.3.16.18.4 Criado em;

5.4 Serviço de Instalação e Configuração da Solução Antivírus, com Treinamento "Hands-On" da Solução de Antivírus

5.4.1 Serviço a ser realizado nas dependências da Superintendência de Tecnologia da Informação, localizada no Térreo do Centro Administrativo, Rua Venâncio Aires, 2277 CEP 97010-005, Centro.

5.4.2 Os serviços técnicos deverão ser realizados por por técnico especializado da própria fabricante e/ou parceiro licenciado, com credenciamento da fabricante.

5.4.3 A Contratante disponibilizará a infraestrutura de servidores (físicos ou virtuais) e os sistemas operacionais necessários para o serviço de instalação e configuração da Solução.

5.4.4 A Contratante não assumirá os custos de licenças e/ou softwares extras, diárias, transporte, assim como outros custos de prestação de serviço no momento desta implantação. Todos os custos devem ser previstos pela CONTRATADA/FABRICANTE da solução na elaboração de sua proposta.

5.4.5 A CONTRATADA deve apresentar um cronograma para a implantação da SOLUÇÃO DE ANTIVÍRUS em até 10 dias úteis após a assinatura do contrato.

5.4.6 O serviço terá a duração de até 15 (quinze) dias úteis. Durante esse período, a equipe da CONTRATADA desenvolverá os trabalhos necessários para a instalação e configuração da Solução de Antivírus sob coordenação de uma equipe técnica da Contratante.

5.4.7 Treinamento Hands-on

5.4.7.1 O curso deve ser ministrado em conjunto com a instalação e configuração do sistema, com a transmissão de conhecimento técnico por parte da CONTRATADA.

5.4.7.2 O curso deve ser ministrado de segunda-feira a sexta-feira em horário de expediente, das 07:30 as 16:30.

5.4.7.3 A CONTRATANTE não assumirá os custos de licenças e/ou softwares extras, diárias e transporte dos instrutores, assim como outros custos relativos a esta capacitação. Todos os custos devem ser previstos pela CONTRATADA na elaboração de sua proposta.

5.4.7.4 CONTRATADA deve transmitir o conhecimento técnico necessário a fim de que os participantes (Equipe Técnica da PMSM) tenham capacidade de conhecer as principais funcionalidades e ferramentas da solução de antivírus implantada na PMSM.

5.4.7.5 O treinamento deve ser de natureza teórica e prática, ser focado no ambiente instalado na Contratante, e deve abordar no mínimo os seguintes tópicos:

5.4.7.5.1 Instalação/Configuração do servidor principal (módulo de gerenciamento central);

5.4.7.5.2 Instalação/Configuração do antivírus no ambiente virtualizado;

5.4.7.5.3 Instalação do software de antivírus em estações de trabalho;

5.4.7.5.4 Operação, descrição e configuração das principais funcionalidades da solução de antivírus;

5.4.7.5.5 Backup e restauração (recovery);

5.4.7.5.6 Resolução de problemas – troubleshooting;

5.4.7.5.7 Melhores práticas utilizadas no mercado para melhor aproveitamento do softwares e de suas funcionalidades.

5.4.7.6 O treinamento deve ser ministrado preferencialmente pelo(s) técnico(s) responsável(is) pela instalação e configuração da solução. Desta forma, há a garantia de que o treinamento seja referente à solução adquirida e de que o instrutor possuirá conhecimento sobre a solução.

5.5 Requisitos para documentação da solução (items 1 e 2)

5.5.1 A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:

5.5.2 Ajuda on-line para administradores

5.5.3 Ajuda on-line para melhores práticas de implementação

5.5.4 Ajuda on-line para proteção de servidores de administração

5.5.5 A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.

5.4.6 Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

5.6 Do serviço gerenciado MXDR (24x7)

5.6.1 O serviço gerenciado MXDR deverá contemplar monitoramento contínuo dos ambientes virtualizados abrangidos pela contratação, em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, incluindo finais de semana e feriados.

5.6.2 O serviço deverá ser executado por equipe especializada de Centro de Operações de Segurança (SOC), compreendendo:

- Monitoramento contínuo dos eventos de segurança dos ambientes protegidos;
- Identificação e análise de atividades suspeitas e potenciais incidentes;
- Investigação e classificação dos incidentes identificados;
- Comunicação dos incidentes à equipe técnica da Contratante;
- Adoção das ações de contenção e resposta previstas no escopo contratado;

- Disponibilização de registros e relatórios das atividades de monitoramento e resposta.

5.6.3 A Contratada deverá disponibilizar mecanismo de acionamento e escalonamento de incidentes, com identificação dos responsáveis e dos procedimentos aplicáveis.

5.6.4 O serviço MXDR deverá permanecer operacional em regime 24x7, independentemente do horário de funcionamento do suporte técnico ordinário previsto neste Termo de Referência.

6. Do Pagamento

6.1 Para os itens 1 e 2: Pagamentos mensais, realizados em até em 30 (trinta) dias corridos contados da apresentação da Nota Fiscal ao fiscal do contrato, acompanhada do ateste da prestação dos serviços.

6.2 Para o item 3: Será realizado um pagamento único após a instalação e homologação da solução de antivírus, em até em 30 (trinta) dias corridos contados da apresentação da Nota Fiscal ao fiscal do contrato, acompanhada do ateste da prestação dos serviços.

6.3 Em caso de reajustes contratuais, os valores serão reajustados anualmente mediante a aplicação da variação do Índice de Custo de Tecnologia da Informação (ICTI), calculado e divulgado pelo IPEA, observadas as diretrizes da Lei nº 14.133/2021.

7. Da Subcontratação

7.1 Será permitida a subcontratação parcial do Lote, para serviços de manutenção presencial e remoto.

7.2 A subcontratação depende de autorização prévia da CONTRATANTE, a quem incumbe avaliar se a subcontratada cumpre os requisitos de qualificação técnica necessários para execução do objeto.

7.3 Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da CONTRATADA pela perfeita execução contratual, cabendo-lhe realizar supervisão e coordenação pelo cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

8. Da Participação de Consórcios

8.1 Não será admitida a participação de consórcios.

9. Critérios de Seleção do Fornecedor

9.1 Apresentar no mínimo 1 (um) Atestado de Capacidade Técnica, emitido por pessoa jurídica de direito público ou privado, que comprove que a empresa já forneceu ou está fornecendo serviço pertinente e compatível com o objeto desta licitação para, no mínimo, 1.000 estações de trabalho.

9.2 Para início do Contrato: Os técnicos responsáveis pelo suporte devem ser capacitados junto ao FABRICANTE da solução através de treinamentos oficiais da mesma comprovada através de certificados de cursos, sendo necessário o cumprimento de, no mínimo, o seguinte requisito:

> 9.2.1 Certificação Oficial do Fabricante ou Declaração do Fabricante de que o profissional está apto a realizar serviço de suporte técnico dos softwares ofertados.

9.3 A exigência de comprovação de experiência anterior em fornecimento ou prestação de serviços compatíveis com, no mínimo, 1.000 estações de trabalho tem por finalidade assegurar que a licitante possua capacidade operacional para atender a um ambiente corporativo de porte relevante, correspondente a 50% do quantitativo previsto para o item, sem exigir experiência prévia na totalidade do objeto contratado.

10. Do Suporte Técnico

10.1 A CONTRATADA deverá prestar suporte técnico na modalidade 8x5 (oito horas por dia, cinco dias por semana, em dias úteis), integralmente incluído na licença contratada, sem qualquer custo adicional para a CONTRATANTE durante toda a vigência contratual.

10.2 O atendimento será realizado exclusivamente por meio de plataforma de chamados (ticket) disponibilizada pela CONTRATADA, na qual todos os chamados abertos pela equipe técnica da CONTRATANTE deverão ficar registrados, permitindo consulta ao histórico, acompanhamento do andamento e emissão de relatórios de atendimento.

10.3 O prazo para atendimento de qualquer chamado registrado na plataforma será de até 8 (oito) horas, contadas a partir do registro do chamado, dentro do horário de funcionamento do suporte (8x5).

10.4 Os contatos para abertura de chamados e agendamentos deverão ser centralizados através da plataforma de chamados da CONTRATADA, podendo ser complementados por e-mail (sti@santamaria.rs.gov.br) quando necessário.

10.5 Em caso de atraso no pagamento por parte da CONTRATANTE superior a 90 (noventa) dias, a CONTRATADA poderá suspender imediatamente a prestação dos serviços objeto deste Termo de Referência, incluindo suporte técnico, atualizações e disponibilização de licenças, até a efetiva regularização dos débitos pendentes pela CONTRATANTE. Regularizados os débitos, os serviços deverão ser restabelecidos imediatamente pela CONTRATADA. A eventual suspensão ou interrupção dos serviços deverá observar os requisitos legais, mediante comunicação formal e prévia à Contratante, considerando especialmente a continuidade dos serviços públicos e os riscos decorrentes da interrupção da proteção dos ativos digitais municipais.

11. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

SABRINA MEDIANEIRA DA SILVA AVILA

Equipe de apoio

Assinou eletronicamente em 04/11/2026 às 10:53:50.