TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

ESTUDO TÉCNICO PRELIMINAR - TJ/AM/SETIC/DVITIC

Responsáveis pela elaboração:

Diogo Mendonça de Sousa

Rafael Araújo da Silva

Contato: (92) 99239-1948

Número de identificação do ETP: 2735870

Categoria do Objeto: Serviços de licenciamento de uso de softwares e suporte técnico

CATSER: 27456

1. PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL

1.1 O objeto da pretensa contratação está previsto no PCA (Plano de Contratações Anual) / 2026, conforme **RESOLUÇÃO Nº 30, DE 11 DE NOVEMBRO DE 2025,** disponibilizado no painel *BI* disponível NESTE LINK, sob o código **SETIC-2026-72**, totalizando **R$ 2.400.000,00** de recurso disponível.

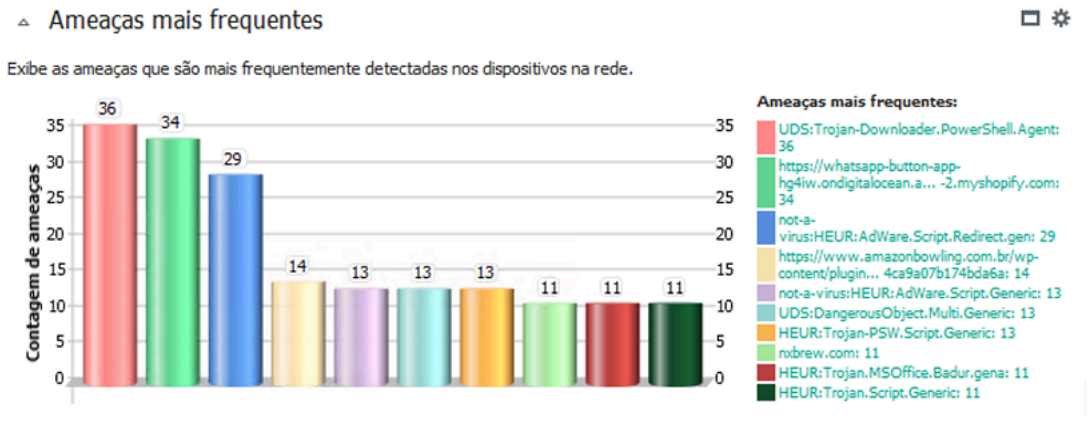
2. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1 Fundamentação e descrição da necessidade da contratação:

Considerando que as licenças do software antivírus atualmente em uso pelo TJAM, bem como os serviços de suporte técnico, terão sua validade expirada em 26/03/2026 e que, consequentemente, passarão a não ter mais atualizações das bases de dados de vírus e correções de erros, os sistemas que dependem dos respectivos softwares passarão a ficar vulneráveis a novas ameaças que surgirem, por isso se faz necessária a aquisição desses softwares em suas versões mais atuais, com o respectivo suporte técnico, para garantir o perfeito funcionamento dos dispositivos que deles são dependentes. Considerando a importância vital que os sistemas e serviços de TI adquiriram para as organizações e a constante diversificação e desenvolvimento de novas ameaças cibernéticas ao longo do tempo, torna-se mandatório o uso de uma solução de antivírus e a disponibilidade de apoio técnico especializado na ferramenta para atingir as metas de segurança da informação, garantir a continuidade dos serviços essenciais e que esteja totalmente alinhada ao ambiente e às melhores práticas de segurança da Informação.

2.2 Evidências técnicas do ambiente em produção:

A necessidade da presente contratação fundamenta-se nas evidências técnicas extraídas da solução de segurança Kaspersky atualmente em produção no ambiente do Tribunal de Justiça do Estado do Amazonas (TJAM). Conforme resultados extraídos da ferramenta de gerenciamento da solução, referente aos últimos 30 (trinta) dias de operação, foram detectadas e bloqueadas diversas tentativas de ameaças cibernéticas, demonstrando a exposição contínua do ambiente institucional a riscos de segurança da informação. Os dados consolidados, apresentados por meio de gráfico ilustrativo, evidenciam a efetividade da solução na mitigação dessas ameaças.



2.3 Evolução e complexidade das ameaças cibernéticas:

Observa-se, de forma contínua, a evolução, diversificação e aumento da complexidade das ameaças cibernéticas, incluindo malwares avançados, ransomwares, ataques direcionados, exploração de vulnerabilidades e tentativas de acesso não autorizado. Tal cenário exige a utilização de soluções de antivírus corporativas robustas, constantemente atualizadas e alinhadas às melhores práticas de segurança da informação, capazes de atuar de forma preventiva, corretiva e reativa diante de incidentes de segurança.

2.4 Padronização, gerenciamento e suporte técnico:

A contratação da solução de antivírus com suporte técnico ativo permitirá manter a padronização do ambiente tecnológico já adotado pelo TJAM, reduzir riscos operacionais e facilitar o gerenciamento centralizado da segurança dos endpoints. Ademais, o suporte técnico especializado é fundamental para auxiliar a equipe interna de TI na correta administração da solução, na rápida resolução de incidentes e na aplicação adequada das políticas de segurança da informação, contribuindo para a continuidade dos serviços essenciais e para a preservação da confidencialidade, integridade e disponibilidade das informações institucionais.

2.11 As normas vigentes aplicáveis a esta contratação incluem, mas não se limitam a:

2.11.1 Lei nº 14.133/2021: Lei de Licitações e Contratos da Administração Pública.

2.11.2 Resolução CNJ nº 468/2022: Diretrizes para contratações de Soluções de Tecnologia da Informação e Comunicação (STIC) pelos órgãos do Poder Judiciário.

2.11.3 Resolução CNJ nº 370/2021: Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

3. UNIDADE DEMANDANTE

3.1 A unidade demandante responsável pelo desenvolvimento e acompanhamento deste estudo será a Secretaria de Tecnologia da Informação e Comunicação - SETIC.

4. REQUISITOS DA CONTRATAÇÃO

4.1 A contratação não é de natureza contínua.

4.2 O contrato terá duração de 36 meses, podendo ser prorrogado nos termos dos arts. 105 e seguintes da Lei n.° 14.133/21.

4.3 Sugere-se que a licitação seja realizada na modalidade Pregão Eletrônico por menor preço global.

4.4 Quando da entrega, a CONTRATADA deverá comprovar, através de acesso ao site do fabricante ou entrega de documentação oficial do fabricante, a aquisição das licenças de software em nome do TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS.

4.5 A entrega das licenças de software deverá ocorrer no prazo máximo de 30 (trinta) dias corridos a contar da assinatura do contrato, podendo ser prorrogado, excepcionalmente, desde que justificado previamente pela CONTRATADA e autorizado pelo CONTRATANTE.

4.6 Considerando a complexidade e o impacto das soluções a serem implantadas, ficam estabelecidos os seguintes requisitos de capacitação técnica, em conformidade com o disposto no art. 67 da Lei nº 14.133/2021, que autoriza a exigência de comprovação de qualificação técnico-profissional e técnico-operacional:

4.6.1 A licitante deverá apresentar Atestado(s) de Capacidade Técnica, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a execução satisfatória de serviços de implantação, configuração e operação de solução de segurança do tipo *Endpoint Protection*, em quantidade mínima de 50% da quantidade objeto deste edital.

4.6.2 Para assegurar a autenticidade, procedência e regularidade técnica da solução de segurança EDR (Endpoint Detection and Response), a licitante deverá apresentar obrigatoriamente, no momento da habilitação, carta de autorização emitida pelo fabricante da solução ofertada, que comprove a qualificação e credenciamento da empresa vencedora junto ao fabricante, citando nominalmente este processo licitatório.

5. LEVANTAMENTO DE MERCADO E JUSTIFICATIVA DA ESCOLHA DO TIPO DE SOLUÇÃO A CONTRATAR

5.1 A necessidade de manter a padronização da infraestrutura de segurança da informação do Tribunal de Justiça do Amazonas (TJAM) justifica a dispensa do levantamento de mercado para esta contratação. O Tribunal utiliza, de forma contínua, desde o ano de 2020, a solução de antivírus corporativo da fabricante Kaspersky, a qual se encontra plenamente integrada ao ambiente tecnológico institucional, atendendo de forma satisfatória aos requisitos de proteção de endpoints, servidores e estações de trabalho. Tal justificativa encontra respaldo no art. 41, inciso I, alíneas “a” e “b”, da Lei nº 14.133/2021, que permite a indicação de marcas e modelos específicos quando necessária a manutenção da padronização e da compatibilidade com soluções já adotadas pela Administração.

5.2 A adoção de solução antivírus distinta da atualmente utilizada poderia acarretar impactos negativos relevantes, tais como aumento dos custos operacionais, necessidade de reconfiguração de políticas de segurança, migração de agentes, readequação de processos internos e capacitação adicional da equipe técnica. Além disso, a substituição da tecnologia vigente poderia comprometer temporariamente o nível de proteção do ambiente computacional, contrariando os princípios da eficiência, da economicidade e da continuidade do serviço público.

5.3 A padronização da solução de antivírus corporativo contribui para a redução da complexidade na administração da segurança da informação, facilita o gerenciamento centralizado, mantém a curva de aprendizado da equipe técnica em patamar adequado e assegura a plena compatibilidade com os sistemas e procedimentos já estabelecidos no TJAM. Esse alinhamento atende ao disposto no art. 47, inciso I, da Lei nº 14.133/2021, que determina a observância do princípio da padronização, visando à compatibilidade técnica e ao desempenho adequado das soluções contratadas.

5.4 A continuidade da utilização da solução Kaspersky minimiza riscos operacionais, preserva a estabilidade do ambiente computacional e garante a manutenção dos níveis de segurança já alcançados, sem a necessidade de adaptações técnicas complexas ou investimentos adicionais desnecessários. Dessa forma, a dispensa do levantamento de mercado se justifica não apenas pela manutenção da padronização tecnológica do TJAM, mas também pelo respaldo legal conferido pela Lei nº 14.133/2021, assegurando eficiência, economicidade e continuidade dos serviços públicos.

5.5 Ressalta-se, ainda, que a solução Kaspersky não se caracteriza como produto de fornecedor exclusivo, sendo comercializada por diversas empresas autorizadas no território nacional. A fabricante mantém um amplo ecossistema de parceiros e revendedores credenciados, o que assegura a competitividade na futura contratação e possibilita à Administração a obtenção da proposta mais vantajosa, afastando qualquer restrição indevida à ampla concorrência.

6. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

6.1 Do módulo de proteção de endpoint

6.1.1 A solução proposta deverá proteger os sistemas operacionais abaixo:
a) Windows 7;
b) Windows 8;
c) Windows 8.1;
d) Windows 10;
e) Windows 11.

6.1.2 Servidores:
a) Windows Small Business Server 2011;
b) Windows MultiPoint Server 2011;
c) Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022.

6.1.3 Servidores de terminal Microsoft:
a) Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022.

6.1.4 Sistemas operacionais Linux de 32 bits:
a) CentOS 6.7 e posterior;
b) Debian GNU/Linux 11.0 e posterior;
c) Debian GNU/Linux 12.0 e posterior;
d) Red Hat Enterprise Linux 6.7 e posterior.

6.1.5 Sistemas operacionais Linux de 64 bits:
a) Amazon Linux 2;
b) CentOS 6.7 e mais tarde;
c) CentOS 7.2 e posterior;
d) CentOS Stream 8;
e) CentOS Stream 9;
f) Debian GNU/Linux 11.0 e posterior;
g) Debian GNU/Linux 12.0 e posterior;
h) Linux Mint 20.3 e superior;
i) Linux Mint 21.1 e posterior;
j) openSUSE Leap 15.0 e posterior;
k) Oracle Linux 7.3 e posterior;
l) Oracle Linux 8.0 e posterior;
m) Oracle Linux 9.0 e posterior;
n) Red Hat Enterprise Linux 6.7 e posterior;
o) Red Hat Enterprise Linux 7.2 e posterior;
p) Red Hat Enterprise Linux 8.0 e posterior;
q) Red Hat Enterprise Linux 9.0 e posterior;
r) Rocky Linux 8.5 e posterior;
s) Rocky Linux 9.1;

t) SUSE Linux Enterprise Server 12.5 ou posterior;
u) SUSE Linux Enterprise Server 15 ou posterior;
v) Ubuntu 20.04 LTS;
w) Ubuntu 22.04 LTS.

6.1.6 Sistemas operacionais Arm de 64 bits:
a) CentOS Stream 9;
b) SUSE Linux Enterprise Server 15;
c) Ubuntu 22.04 LTS.

6.1.7 Sistemas operacionais MAC OS:
a) macOS 12 – 14.

6.1.8 Ferramentas de virtualização MAC OS:
a) Parallels Desktop 16 para Mac Business Edition ou superior;
b) VMware Fusion 11.5 Profissional ou superior.

6.1.9 A solução proposta deverá suportar as seguintes plataformas virtuais:
a) VMware Workstation;
b) VMware ESXi;
c) Microsoft Hyper-V Server;
d) Citrix Virtual Apps e Desktop;
e) Citrix Provisioning.

6.2 Do módulo de gerenciamento avançado

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

6.2.2 A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
a) Amazon Web Services;
b) Microsoft Azure;
c) Google Cloud.

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

6.2.4 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.

6.2.5 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.

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

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

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

6.2.9 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.

6.2.10 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.

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

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

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

6.2.14 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:
a) Status do dispositivo;
b) Tag;
c) Diretório ativo;
d) Proprietários de dispositivos;
e) Hardware.

6.2.15 A solução proposta deve suportar os seguintes canais de entrega de notificação:
a) E-mail;
b) Registro de sistema;
c) SMS.

6.2.16 A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:
a) Atributos de rede;
b) Nome;
c) Domínio e/ou Sufixo de Domínio;
d) Endereço de IP;
e) Endereço IP para servidor de gerenciamento;
f) Localização no Active Directory;
g) Unidade organizacional;
h) Grupo;
i) Sistema operacional;
j) Número do pacote de serviço;
k) Arquitetura Virtual;
l) Registro de aplicativos;
m) Nome da Aplicação;
n) Versão do aplicativo;
o) Fabricante;
p) Tipo e versão;
q) Arquitetura.

6.2.17 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.

6.2.18 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.

6.2.19 As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:
a) Dispositivos Desktop/Servidores;
b) Dispositivos móveis;
c) Dispositivos de rede;
d) Dispositivos virtuais;
e) Componentes OEM;
f) Periféricos de computador;
g) Dispositivos IoT conectados;
h) Telefones VoIP;
i) Repositórios de rede.

6.2.20 A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:
a) Nome da Aplicação;
b) Caminho do aplicativo;
c) Metadados do aplicativo;
d) Aplicativo Certificado digital;
e) Categorias de aplicativos predefinidas pelo fornecedor;
f) SHA256 e MD5.

6.2.21 A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:
a) Bluetooth;
b) Dispositivos móveis;
c) Modems externos;
d) CD/DVD;
e) Câmeras e scanners;
f) MTPs;
g) E a transferência de dados para dispositivos móveis.

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

6.2.23 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.

6.2.24 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:
a) Estruturas de domínios e grupos de trabalho do Windows;
b) Estruturas de grupos do Active Directory;
c) Conteúdo de um arquivo de texto criado manualmente pelo administrador.

6.2.25 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.

6.2.26 A solução proposta deve permitir realizar as seguintes ações para endpoints:
a) Verificação manual;
b) Verificação no acesso;
c) Verificação por demanda;
d) Verificação de arquivos compactados;
e) Verificação de arquivos individuais, pastas e unidades;
f) Bloqueio e verificação de scripts;
g) Proteção contra alteração de registros;
h) Proteção contra estouro de buffer;
i) Verificação em segundo plano/inativa;
j) Verificação de unidade removível na conexão com o sistema.

6.2.27 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.

6.2.28 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.

6.2.29 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.

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

6.2.31 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.

6.2.32 A solução proposta deve suportar Windows Failover Cluster.

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

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

6.2.35 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.

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

6.2.37 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.

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

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

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

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

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

6.2.43 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 específico de prevenção de intrusão.

6.2.44 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.

6.2.45 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).

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

6.2.47 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.

6.2.48 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.

6.2.49 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.

6.2.50 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.

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

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

6.2.53 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.

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

6.2.55 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.

6.2.56 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.

6.2.57 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.

6.2.58 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.

6.2.59 A solução proposta deve permitir ao administrador personalizar relatórios.

6.2.60 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.

6.2.61 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.

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

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

6.2.64 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.

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

6.2.66 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.

6.2.67 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.

6.2.68 A solução proposta deve suportar integração com solução APT.

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

6.2.70 A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
a) Windows;
b) Linux.

6.2.71 A solução proposta deverá suportar os seguintes servidores de banco de dados:
a) Windows: Microsoft SQL Server; Microsoft Banco de dados SQL do Azure; MySQL Standard e Enterprise; MariaDB; PostgreSQL.
b) Linux: MySQL; MariaDB; PostgreSQL.

6.2.72 A solução proposta deverá suportar as seguintes plataformas virtuais:
a) Windows: VMware vSphere 6.7 e 7.0; Estação de trabalho VMware 16 Pro; Servidor Microsoft Hyper-V 2012 de 64 bits; Servidor Microsoft Hyper-V 2012 R2 de 64 bits; Microsoft Servidor Hyper -V 2016 de 64 bits; Servidor Microsoft Hyper-V 2019 de 64 bits; Servidor Microsoft Hyper-V 2022 de 64 bits; Citrix XenServer 7.1 LTSR; Citrix XenServer 8.x; Oracle VM VirtualBox 6.x.
b) Linux: VMware vSphere 6.7 e 7.0; VMware Desktop 16 Pro e 17 Pro; Servidor Microsoft Hyper-V 2012 de 64 bits; Servidor Microsoft Hyper-V 2012 R2 de 64 bits; Microsoft Servidor Hyper -V 2016 de 64 bits; Servidor Microsoft Hyper-V 2019 de 64 bits; Servidor Microsoft Hyper-V 2022 de 64 bits; Citrix XenServer 7.1 e 8.x; Oracle VM VirtualBox 6.x e7.x.

6.2.73 A solução proposta deve suportar criptografia em vários níveis:
a) Criptografia completa do disco – incluindo disco do sistema;
b) Criptografia de arquivos e pastas;
c) Criptografia de mídia removível;
d) Gerenciamento de criptografia BitLocker e MacOS Filevault2.

6.2.74 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
a) A criptografia de arquivos em unidades de computador locais;
b) A criação de listas de criptografia de arquivos por extensão ou grupo de extensões;
c) A criação de listas criptografadas de pastas em unidades de computador locais.

6.2.75 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:
a) Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis;
b) Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

6.2.76 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:

a) A criptografia de todos os arquivos armazenados em unidades removíveis;
b) A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.

6.2.77 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.

6.2.78 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.

6.2.79 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.

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

6.2.81 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.

6.2.82 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.

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

6.2.84 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.

6.2.85 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.

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

6.2.87 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.

6.2.88 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.

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

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

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

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

6.2.93 A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:
a) Uso do Trusted Platform Module e configurações de senha;
b) Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível;
c) 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).

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

6.2.95 A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
a) Instalação remota de software de terceiros;
b) Relatórios sobre software e hardware existentes;
c) Monitoramento para instalação de software não autorizado;
d) Remoção de software não autorizado.

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

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

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

6.2.99 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.

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

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

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

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

6.2.104 A solução proposta deve permitir ao administrador aprovar atualizações.

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

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

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

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

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

6.2.110 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).

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

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

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

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

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

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

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

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

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

6.2.120 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.

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

6.2.122 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.

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

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

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

6.2.126 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.

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

6.2.128 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.

6.2.129 A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
a) Inicie a instalação ao reiniciar ou desligar o computador;
b) Instale o gerador necessário todos os pré-requisitos do sistema;
c) Permitir a instalação de novas versões de aplicativos durante as atualizações;
d) Baixe atualizações para o dispositivo sem instalá-las.

6.2.130 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.

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

6.2.132 O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
a) CEF;
b) LEEF.

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

6.2.134 O relatório da solução proposta deve conter informações CVE.

6.2.135 A solução proposta deve suportar instalação de aplicações e software de terceiros.

6.3 Do módulo de gerenciamento simplificado

6.3.1 A solução proposta deve suportar arquitetura cloud.

6.3.2 A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

6.3.3 O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

6.3.4 A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

6.3.5 A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

6.3.6 A solução proposta deve atender as condições apontadas no item e subintes 6.

6.3.7 A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

6.3.8 A solução proposta deve incluir informações do endpoint:
a) IP público de internet;
b) IP interno do dispositivo;
c) Versão do agente de proteção;
d) Ultima comunicação com a console, contendo data e hora;
e) Informações do sistema operacional.

6.3.9 A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.

6.3.10 A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.

6.3.11 A solução proposta deve incluir treinamento em segurança cibernética.

6.4 Requisitos gerais

6.4.1 A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
a) 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.

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

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

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

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

6.4.6 A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
a) Proteção contra ameaças sem arquivos (Fileless);
b) Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque.

6.4.7 A solução proposta deve fornecer varredura de memória para estações de trabalho Windows.

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

6.4.9 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.

6.4.10 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.

6.4.11 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.

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

6.4.13 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.

6.4.14 A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
a) Controles de aplicativos;
b) Controle web e dispositivos;
c) HIPS e Firewall;
d) Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
e) Gerenciamento de criptografia de arquivos e discos;
f) Controle adaptativo para detecção de anomalias.

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

6.4.16 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.

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

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

6.4.19 A solução proposta deve incluir um módulo capaz, no mínimo, de:
a) Bloqueio de aplicativos com base em sua categorização;
b) Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos;
c) A adição de sub-redes e a modificação de permissões de atividade.

6.4.20 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.

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

6.4.22 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.

6.4.23 A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
a) Modo silencioso;
b) Discos rígidos e dispositivos removíveis;
c) De todos as contas de usuários do dispositivo.

6.4.24 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
a) Exclusão imediata de dados;
b) Exclusão de dados adiada.

6.4.25 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
a) Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
b) Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

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

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

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

6.4.29 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.

6.4.30 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.

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

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

6.4.33 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.

6.4.34 A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho.

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

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

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

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

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

6.4.40 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.

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

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

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

6.4.44 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.

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

6.4.46 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.

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

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

6.4.49 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.

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

6.4.51 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.

6.4.52 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.

6.4.53 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.

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

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

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

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

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

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

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

6.4.61 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.

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

6.4.63 A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
a) Filtro de anexos;
b) Verificação de mensagens de email ao receber, ler e enviar.

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

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

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

6.4.67 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.

6.4.68 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.

6.4.69 A solução proposta deve incluir suporte ao protocolo IPv6.

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

6.4.71 A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
a) Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo;
b) Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

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

6.4.73 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.

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

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

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

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

6.4.78 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.

6.4.79 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.

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

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

6.4.82 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.

6.4.83 A solução proposta deve suportar endereços IPv6.

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

6.4.85 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.

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

6.4.87 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.

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

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

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

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

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

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

6.4.94 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.

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

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

6.4.97 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.

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

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

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

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

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

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

6.4.104 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.

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

6.4.106 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.

6.4.107 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.

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

6.4.109 A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
a) Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível;
b) Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

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

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

6.5 Do modulo de gerenciamento de dispositivos móveis

6.5.1 O modulo deve ser integrado a console de gerenciamento.

6.5.2 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
a) Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition).

6.5.3 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
a) iOS 10–17 ou iPadOS 13–17.

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

6.5.5 A solução proposta deve suportar dispositivos iOS supervisionados.

6.5.6 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.

6.5.7 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.

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

6.5.9 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).

6.5.10 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.

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

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

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

6.5.14 A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
a) Dados em contêineres;
b) Contas de e-mail corporativo;
c) Configurações para conexão à rede Wi-Fi corporativa e VPN;
d) Nome do ponto de acesso (APN);
e) Perfil do Android for Work;
f) Recipiente KNOX;
g) Chave do gerenciador de licença KNOX.

6.5.15 A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
a) Todos os perfis de configuração instalados;
b) Todos os perfis de provisionamento;
c) O perfil iOS MDM;
d) Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas.

6.5.16 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.

6.5.17 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:
a) Critérios de verificação do dispositivo;
b) Prazo 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.

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

6.5.19 A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
a) Cartões de memória e outras unidades removíveis;
b) Câmera do dispositivo;
c) Conexões Wi-Fi;
d) Conexões Bluetooth;
e) Porta de conexão infravermelha;
f) Ativação do ponto de acesso Wi-Fi;
g) Conexão de área de trabalho remota;
h) Sincronização de área de trabalho;
i) Definir configurações da caixa de correio do Exchange;
j) Configurar caixa de e-mail em dispositivos iOS MDM;
k) Configure contêineres Samsung KNOX;

l) Definir as configurações do perfil do Android for Work;
m) Configurar e-mail/calendário/contatos;
n) Defina as configurações de restrição de conteúdo de mídia;
o) Definir configurações de proxy no dispositivo móvel;
p) Configurar certificados e SCEP.

6.5.20 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.
a) Portal de inscrição móvel KNOX;
b) Pacotes de instalação pré-configurados independentes.

6.5.21 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.

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

6.5.23 A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
a) VMware AirWatch 9.3 ou posterior;
b) MobileIron 10.0 ou posterior;
c) IBM MaaS360 10.68 ou posterior;
d) Microsoft Intune 1908 ou posterior;
e) SOTI MobiControl 14.1.4 (1693) ou posterior.

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

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

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

6.5.27 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.

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

6.5.29 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.

6.5.30 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.

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

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

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

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

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

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

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

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

6.6 Do módulo de EDR

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

6.6.2 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.

6.6.3 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.

6.6.4 Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise.

6.6.5 Deve apresentar informações detalhadas contendo:
a) Usuário que executou a ação;
b) Informações acesso privilegiado.

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

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

6.6.8 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.)

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

6.6.10 Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas.

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

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

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

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

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

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

6.6.17 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.

6.6.18 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.

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

6.6.20 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:
a) Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque);
b) Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional;

c) Informações gerais sobre a detecção, incluindo modo de detecção;
d) Alterações no registro associadas à detecção;
e) Histórico da presença de arquivos no dispositivo;
f) Ações de resposta executadas pela aplicação.

6.6.21 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.

6.6.22 A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
a) Processo;
b) Conexões de rede;
c) Alterações no registro;
d) Detalhes do download de objeto.

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

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

6.6.25 A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
a) Impedir a execução de objetos;
b) Isolamento de host;
c) Excluir objeto do host ou grupo de hosts;
d) Encerrar um processo no dispositivo;
e) Colocar um objeto em quarentena;
f) Execute a verificação do sistema;
g) Execução remota de programa/processo/comando;
h) Iniciar a varredura IoC para um grupo de hosts.

6.7 Requisitos para documentação da solução.

6.7.1 A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
a) Ajuda on-line para administradores;
b) Ajuda on-line para melhores práticas de implementação;
c) Ajuda on-line para proteção de servidores de administração.

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

6.7.3 Deve estar disponível página com informações de ciclo de vida das soluções e módulos.

6.8 **SERVIÇOS DE CONSULTORIA E SUPORTE ESPECIALIZADO**

6.8.1. Serviços de Suporte Técnico Especializado e Consultoria para Plataforma Kaspersky, que deverão ser prestados através de Banco de Horas (120h):

6.8.1.1. A CONTRATADA prestará serviços de consultoria e suporte técnico especializado nas soluções Kaspersky implantadas na CONTRATANTE, com foco em proteção de endpoints e funcionalidades EDR.

6.8.1.2. Os serviços serão realizados por meio de um banco de 120(cento e vinte) horas técnicas, disponibilizadas ao longo da vigência contratual, mediante solicitação da CONTRATANTE.

6.8.2. Das condições de execução dos serviços:

6.8.2.1. As horas poderão ser utilizadas sob demanda, mediante solicitação formal da CONTRATANTE, via chamado telefônico ou e-mail, entre 9h e 18h, de segunda a sexta-feira (horário de Brasília);

6.8.2.2. Os serviços poderão ser executados remotamente;

6.8.2.3. O suporte incluirá:

6.8.2.3.1. Esclarecimento de dúvidas de utilização, administração e operação das soluções Kaspersky fornecidas;

6.8.2.3.2. Orientação sobre atualizações, correções e melhorias;

6.8.2.3.3. Envio de procedimentos e boas práticas para operação segura e eficiente da solução;

6.8.2.3.4. Apoio em incidentes e contenção de ameaças;

6.8.2.3.5. Auditoria, revisão e análise de logs.

6.8.3. Da abrangência dos serviços de consultoria:

6.8.3.1. Os serviços contemplam, entre outros:

6.8.3.1.1. Análise, planejamento e implantação de projetos relacionados a soluções antivírus, EDR e proteção em nuvem Kaspersky;

6.8.3.1.2. Auxílio na gestão de políticas de segurança, incluindo prevenção e combate a ameaças como vírus, spywares, ransomwares e rootkits;

6.8.3.1.3. Avaliação de vulnerabilidades e recomendações de mitigação;

6.8.3.1.4. Instalação e configuração de atualizações de versão e patches;

6.8.3.1.5. Parametrização de filtros, regras e mecanismos de bloqueio para ameaças sem vacina;

6.8.3.1.6. Apoio na análise de logs e investigação de eventos de segurança.

6.8.4. Das condições operacionais e SLA:

6.8.4.1. O suporte será prestado por equipe com certificação oficial Kaspersky;

6.8.4.2. O atendimento ocorrerá em regime 8x5 com tempos de resposta conforme prioridade: a) Conforme tabela de SLA no item 6.8.6.

6.8.5. Da gestão e controle do banco de horas:

6.8.5.1. A CONTRATADA enviará até o dia 10 de cada mês o extrato das horas utilizadas no mês anterior;

6.8.5.2. A CONTRATANTE terá até 5 (cinco) dias úteis para validar ou contestar os relatórios enviados;

6.8.5.3. A CONTRATADA poderá emitir Nota Fiscal somente após o aceite das horas executadas.

6.8.5.4. O pagamento das horas será efetuado no prazo máximo de até 30 (trinta) dias, podendo ser de forma integral ou parcelada, através de conta corrente da CONTRATADA, no banco e conta corrente por ela indicados pela contratada.

6.8.6. Disposições finais

6.8.6.1. Este serviço não substitui a implantação inicial das soluções já contempladas nos documentos técnicos de EDR Optimum;

6.8.6.2. O banco de horas é válido durante a vigência contratual e pode ser utilizado conforme necessidade da CONTRATANTE.

DUVIDA	SOLICITAÇÃO DE SERVIÇOS	INCIDEN

PADRÃO	PADRÃO	CRÍTICO	ALTO
Primeiro atendimento em até: 08 horas	Primeiro atendimento em até: 04 horas	Primeiro atendimento em até: 01 hora	Primeiro atendimento em até: 04 horas
Tempo para resolução em até: 72 horas	Tempo para resolução em até: 48 horas	Tempo para solução ou contorno em até: 04 horas	Tempo para solução ou contorno em até: 0 horas
Solicitações de dúvida sobre a plataforma ou sobre os serviços contratados.	Solicitações de novos serviços relacionado s ao produto contratado, como exemplo: Novas configurações, novos relatórios, novas parametrizações, entre outros.	Incidente crítico que paralise totalmente os serviços do ambiente de produção com impacto direto no negócio.	Incidente grave que prejudique a operação d solução ou limite severamente suas funcionalidades com a paralisação parcial d serviço.

7. DA NECESSIDADE DE FORMALIZAÇÃO DE CONTRATO

7.1 Deverá ser formalizado contrato para os serviços previstos neste Estudo Técnico Preliminar (ETP), tendo em vista as características do objeto a ser contratado, com a existência de obrigações futuras, incluindo a garantia, continuidade e confiabilidade do mesmo.

7.2 Não é admitida a subcontratação do objeto contratual.

8. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

8.1 Atualmente, o Tribunal de Justiça do Estado do Amazonas (TJAM) utiliza aproximadamente 4.000 (quatro mil) licenças da solução de antivírus corporativo, quantidade necessária para atender à proteção das estações de trabalho, servidores e demais dispositivos computacionais em operação no ambiente institucional.

8.2 A estimativa atual considera o parque tecnológico existente, abrangendo equipamentos utilizados nas atividades administrativas e jurisdicionais, distribuídos entre a sede, fóruns, comarcas do interior e demais unidades vinculadas ao TJAM.

8.3 Considerando a expansão gradual do parque tecnológico do Tribunal, decorrente da ampliação de unidades administrativas, modernização de equipamentos, substituição de ativos obsoletos e eventual incremento de novos serviços e sistemas informatizados, projeta-se um crescimento na quantidade de dispositivos que necessitarão de proteção ao longo do período contratual.

8.4 Diante desse cenário, estima-se necessária a contratação de 5.000 (cinco mil) licenças da solução de antivírus, quantidade que contempla uma margem de crescimento planejada, permitindo absorver novas demandas sem a necessidade de aditivos contratuais ou novas contratações durante a vigência do contrato.

Item	Descrição	Unidade	Quantidade
01	Fornecimento de Licença de uso do software antivírus KASPERSKY NEXT EDR OPTIMUM, com suporte técnico, por 36 meses.	Unidade	5000
02	Serviços Especializados para SUPORTE TÉCNICO E CONSULTORIA	Horas	120

9. ESTIMATIVA DE PREÇOS

9.1.

Item	Descrição	Unidade	Quantidade	Valor Estimado Unitário	Valor Estimado Anual
1	Fornecimento de Licença de uso do software antivírus KASPERSKY NEXT EDR OPTIMUM, com suporte técnico, por 36 meses.	Unidade	5000	R$ 465,60	R$ 2.328.000,00
2	Serviços Especializados para SUPORTE TÉCNICO E CONSULTORIA	Hora	120	R$ 600,00	R$ 72.000,00
				TOTAL	**R$ 2.400.000,00**

10. JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

10.1 Não se aplica, pois trata-se de um item único.

11. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

11.1 A contratação proveniente deste ETP visa substituir o Contrato Administrativo 005/2023-FUNJEAM.

12. RESULTADOS PRETENDIDOS

12.1 Garantir a proteção contínua dos ativos de Tecnologia da Informação do Tribunal de Justiça do Estado do Amazonas (TJAM) contra ameaças cibernéticas, tais como vírus, malwares, ransomwares e demais códigos maliciosos, por meio da utilização de solução de antivírus corporativa atualizada e reconhecida no mercado.

12.2 Assegurar a manutenção da confidencialidade, integridade e disponibilidade das informações institucionais, reduzindo os riscos de vazamento de dados, indisponibilidade de sistemas e comprometimento de informações sensíveis.

12.3 Manter a continuidade e a estabilidade dos serviços informatizados utilizados nas atividades administrativas e jurisdicionais do TJAM, evitando interrupções decorrentes de incidentes de segurança da informação.

12.4 Proporcionar gerenciamento centralizado da segurança dos endpoints, permitindo maior controle, visibilidade e padronização das políticas de segurança aplicadas a estações de trabalho, servidores e demais dispositivos conectados à rede institucional.

12.5 Reduzir o impacto operacional e o tempo de resposta a incidentes de segurança da informação, por meio de mecanismos avançados de detecção, resposta e mitigação de ameaças, aliados ao suporte técnico especializado da solução contratada.

12.6 Minimizar custos operacionais e riscos associados à ocorrência de incidentes de segurança, evitando gastos extraordinários com recuperação de sistemas, restauração de dados e mitigação de danos decorrentes de ataques cibernéticos.

12.7 Garantir a conformidade do ambiente tecnológico do TJAM com as melhores práticas de segurança da informação e com as diretrizes institucionais, contribuindo para o atendimento às normas internas, à legislação vigente e às recomendações dos órgãos de controle.

12.8 Preservar a padronização tecnológica já adotada pelo Tribunal, reduzindo a complexidade da administração do ambiente de TI e a necessidade de capacitação adicional da equipe técnica em soluções distintas.

13. PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO

13.1 O objeto deste ETP não enseja nenhuma adequação no ambiente.

14. IMPACTOS AMBIENTAIS

14.1 Aplicar, no que couber, a Resolução CNJ nº 400 de 16 de junho de 2021 que dispõe sobre a política de sustentabilidade no âmbito do Poder Judiciário.

15. SERVIÇOS DE MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

15.1 Os Serviços de Manutenção e Suporte Técnicos estão evidenciados no Item 6.8

16. DECLARAÇÃO DE VIABILIDADE (OU NÃO) DA CONTRATAÇÃO

16.1 Considerando todo o exposto, a Secretaria de Tecnologia da Informação e Comunicação (SETIC), por meio da Divisão de Infraestrutura de TIC (SETIC/DVITIC), declara que a contratação de uma solução de proteção de endpoints contra softwares maliciosos é viável e indispensável para garantir a segurança, a integridade e a disponibilidade dos serviços jurisdicionais e administrativos essenciais do TJAM.

17. OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS

17.1 O objeto desta pretensa contratação, por si só, não está diretamente vinculada à Lei Geral de Proteção de Dados (LGPD). Portanto, esta aquisição não exige cláusulas específicas de proteção de dados.

18. MAPEAMENTO DE RISCOS

FASE: ESTUDO TÉCNICO PRELIMINAR										
ID	**CAUSA (DEVIDO A)**	**EVENTO (PODERÁ OCORRER)**	**CONSEQUÊNCIA (O QUE PODERÁ LEVAR A)**	**PROB.**	**IMPACTO**	**NÍVEL**	**RESPOSTA**	**MEDIDAS PREVENTIVAS (PARA EVITAR QUE OCORRA)**	**MEDIDAS DE CONTINGÊNCIA (SE OCORRER, O QUE DEVE SER FEITO)**	**RESPONSÁVEL**
R1	Falta de alinhamento entre a necessidade e o escopo técnico do ETP	Elaboração de requisitos técnicos incompletos ou divergentes	Atrasos na contratação e necessidade de revisão do ETP	3	4	Alto	Revisar constantemente os requisitos	Reuniões de alinhamento entre a SETIC e as unidades demandantes	Ajustar rapidamente os requisitos técnicos	SETIC
R2	Subestimação dos custos e da abrangência da solução	Estimativas de valores abaixo dos preços praticados no mercado	Restrição orçamentária e necessidade de revisão do estudo técnico	2	4	Moderado	Revisão detalhada das estimativas de custo	Pesquisa de preços de mercado atualizada e ampla	Readequar o escopo e as estimativas orçamentárias	SETIC
R3	Incompleta identificação das necessidades institucionais	Definição inadequada do objeto da contratação	Necessidade de reabertura do processo ou revisão do ETP	1	4	Baixo	Revisão da descrição das necessidades	Consulta ampla às áreas usuárias e análise do planejamento estratégico	Ajustar o objeto da contratação antes da conclusão do ETP	SETIC

NÍVEL DE RISCO

Alto: Obrigatoriedade de tratamento do risco por meio de ação, monitoramento, e controle efetivo.

Moderado: Recomendável o tratamento do risco por meio de ação, monitoramento, e controle.

Baixo: Não há obrigatoriedade de tratamento do risco, cabendo uma reavaliação no ciclo posterior e/ou decisão da alta direção do TJAM quanto à emissão de ação, após a análise do tema em questão.

Baixo	**Menor e/ou igual a 5.**
Moderado	**Entre 6 e 9.**
Alto	**Maior que 9.**

Manaus- AM, data registrada no sistema.

Rafael Araújo da Silva	**Diogo Mendonça de Sousa**	**Breno Figueiredo Corado**
Fiscal Técnico do Contrato Administrativo 005/2023-FUNJEAM SETIC/DVITIC	Diretor da Divisão de Infraestrutura de TIC SETIC/DVITIC	Secretário de Tecnologia da Informação e Comunicação SETIC

Documento assinado eletronicamente por **Rafael Araújo da Silva**, **Servidor**, em 04/03/2026, às 14:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DIOGO MENDONCA DE SOUSA**, **Diretor(a)**, em 04/03/2026, às 14:35, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRENO FIGUEIREDO CORADO**, **Secretário(a)**, em 04/03/2026, às 15:23, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjam.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2735870** e o código CRC **5975A851**.