INSTITUTO DE GEO-CIENCIAS/UFMG

Estudo Técnico Preliminar 5/2026

1. Informações Básicas

Número do processo: 23072.225993/2026-20

2. Descrição da necessidade

O presente estudo tem por finalidade demonstrar a necessidade de contratação e renovação da licença do software antivírus, visando à proteção e segurança dos computadores do Instituto de Geociências da UFMG, em atendimento às demandas do Setor de Tecnologia da Informação.

A contratação objetiva assegurar a continuidade e atualização da infraestrutura de segurança da informação da unidade, garantindo proteção contra ameaças cibernéticas, gestão centralizada de dispositivos, criptografia de dados e conformidade com normas técnicas aplicáveis, como a ISO 27001.

No momento, faz-se necessária a aquisição de 100 licenças, destinadas tanto às máquinas dos setores administrativos (incluindo a Casa da Glória, em Diamantina) quanto aos laboratórios utilizados pelos discentes.

A renovação do Software Eset Protect Entry, justifica-se pela necessidade contínua de manutenção da segurança cibernética, bem como pelo fato de o referido software já ter sido contratado em períodos anteriores, encontrando-se instalado e em uso para proteção dos equipamentos do IGC.

Para subsidiar a decisão, foi realizada pesquisa de mercado com solicitação de cotação do software, especificamente para fins de renovação da licença existente, de modo a garantir a manutenção e a continuidade da proteção do parque tecnológico da unidade.

O objetivo da contratação tem por finalidade a renovação da licença de software pelo período de cinco anos. A opção por este prazo mostra-se mais vantajosa para a Administração Pública, conforme demonstrado nos orçamentos anexados ao processo, uma vez que proporciona redução significativa no custo anual da licença.

De acordo com os valores apresentados pelo solicitante, a contratação pelo período de cinco anos implicaria em um custo anual de **R$ 4.586,11** por licença, ao passo que a contratação pelo período de três anos resultaria em um custo anual de **R$ 5.506,47**. A diferença entre os valores evidencia uma economia aproximada de **R$ 920,36 por ano**, reforçando a racionalidade econômica da escolha pelo prazo mais longo.

Dessa forma, a contratação por cinco anos atende ao princípio da economicidade e assegura melhor aproveitamento dos recursos públicos, justificando a adoção desta alternativa.

3. Área requisitante

Área Requisitante	Responsável
Setor de Tecnologia da Informação	Vinícius Etrusco Moreira

4. Necessidades de Negócio

A contratação em questão compõe solução que visa atender demandas relacionadas ao Setor de Tecnologia da Informação, como objetivo estratégico do Instituto de Geociências/UFMG previsto no PCA 2026, formalizado no DFD 22/2026.

O Setor de Tecnologia da Informação visa, assim:

* Garantir a atualização e adequação da infraestrutura, sistemas e serviços de TIC;

* Garantir a disponibilidade de sistemas e serviços de TIC essenciais ao IGC;

* Promover a segurança da informação e a proteção avançada para todo o armazenamento de arquivo de rede, servidores gerais e servidores multiuso;

* Fornece Proteção contra ataques direcionados, contra ransomware, contra ataques sem arquivo e também oferecer gerenciamento remoto e unificado;

* Assegurar que os servidores fiquem estáveis e livres de conflito;

* Limitar reinicializações e janelas de manutenção a um mínimo para garantir a continuidade das atividades.

5. Necessidades Tecnológicas

A renovação da solução de segurança Eset Protect Entry será conduzida pelo Setor de Tecnologia da Informação (STI), abrangendo um total de 100 licenças, destinadas às estações de trabalho administrativas dos servidores e ao laboratório de informática utilizado pelos discentes. A vigência será de 60 meses, assegurando proteção em tempo real dos componentes, serviços e informações que integram o parque computacional do Instituto de Geociências da UFMG.

A solução vigente da ESET proporciona proteção em múltiplas camadas para os equipamentos atendidos, sem comprometer o desempenho dos dispositivos. Além disso, como em todos os produtos corporativos da empresa, está incluída a ferramenta de gestão centralizada, que garante visibilidade completa da rede e possibilita a implementação de medidas corretivas de forma remota e unificada.

O nível de segurança oferecido pelas tecnologias da ESET apresenta impacto mínimo nos sistemas, permitindo a manutenção do desempenho dos dispositivos. Dessa forma, eventuais incidentes na rede podem ser solucionados de imediato, evitando perda de dados e interrupções nas atividades da unidade.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

A escolha pela solicitação de contratação do software Eset Protect Entry justifica-se pelo fato de que os equipamentos que receberão a continuidade da proteção já se encontram atualmente instalados e resguardados por esta solução. Dessa forma, os serviços contratados deverão ser disponibilizados para instalação e uso na unidade a partir de **1º de julho de 2026**, imediatamente após o término da vigência da licença atualmente em uso.

O Setor de Tecnologia da Informação solicita a renovação pelo período de cinco anos, abrangendo 100 licenças, considerando que a contratação por prazo superior a três anos apresenta melhor relação custo-benefício e maior vantagem para a Administração. Ressalta-se que os equipamentos do parque tecnológico não podem permanecer desprotegidos, sob risco iminente de ataques cibernéticos que poderiam ocasionar prejuízos significativos ao patrimônio tecnológico do Instituto de Geociências.

A empresa contratada deverá assegurar:

- fornecimento de suporte técnico durante todo o período de vigência da licença;
- entrega de softwares originais;
- substituição imediata em caso de defeito, irregularidade ou desacordo com a proposta;
- disponibilização de todas as atualizações e inovações do software;
- suporte técnico on-line durante todo o período contratual.

7. Estimativa da demanda - quantidade de bens e serviços

A estimativa do quantitativo total de 100 unidades da licença do software foi definida com base na quantidade do numero de maquinas que se encontram hoje protegidas pelo Antivírus e tem vigência programada para se encerrar em 30 de junho de 2026. As licenças foram lançadas no Planejamento Anual de Contratações do Instituto de Geociências e são descritas conforme as condições e quantidades estabelecidas na tabela abaixo:

ITEM	C O D . SIASG	QUANTIDADE	DESCRIÇÃO/ESPECIFICAÇÃO	P R E Ç O UNITÁRIO	PREÇO TOTAL
1	27502	100	Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software - ESET PROTECT ENTRY - Renovação da Licença por 60 meses.	R$229,30	R$22.930,56
VALOR TOTAL DA CONTRATAÇÃO				R$ 22.930,56	

8. Levantamento de soluções

Para dar seguimento com as avaliações das soluções disponíveis é necessário que se sigam três passos durante a elaboração de um estudo técnico preliminar:

1. A busca de soluções que estejam em utilização por outros órgãos públicos para cessão;

2. A procura por software que desempenhe a função desejada no portal do software público;

3. A busca em soluções disponíveis no mercado.

O software objeto deste estudo, uma solução corporativa de antivírus multiplataforma com gerenciamento centralizado, caracteriza-se por sua alta complexidade e múltiplas funcionalidades incorporadas. Trata-se de produto não desenvolvido sob encomenda, mas adquirido mediante licenciamento, exigindo atualizações periódicas — sendo comum a disponibilização de mais de uma atualização por dia.

Diante desse cenário, a busca por outro órgão público que pudesse ceder solução semelhante não apresentou resultados positivos, uma vez que as licenças são exclusivas para os respectivos contratantes. Em seguida, foi realizada consulta ao Portal do Software Público Brasileiro (https://softwarepublico.gov.br), que disponibiliza softwares livres voltados à modernização da Administração Pública, compartilhados sem ônus e com potencial de gerar economia de recursos.

Todavia, nas pesquisas realizadas no referido portal, não foram identificadas soluções livres que atendam às necessidades específicas do Instituto de Geociências. Em razão desse resultado negativo, as alternativas concentram-se em soluções disponíveis no mercado, que possam garantir a continuidade da proteção e da segurança da infraestrutura tecnológica da unidade.

9. Análise comparativa de soluções

Com vista a verificar os fabricantes e fornecedores de solução corporativa de antivírus, no quesito de proteção, performance e usabilidade, abaixo seguem dois levantamentos realizados pela instituição AV-TEST,(https://www.av-test.org) conhecida mundialmente por avaliar soluções de antivírus de diversos fabricantes. Ela apresenta periodicamente comparativos entre diversas soluções em versões para usuários domésticos (home users) e também as destinadas a empresas (business users).

Para o presente estudo foram consideradas as versões destinadas a uso empresarial.

Ainda sobre os testes mencionados acima, cabe destacar os seus respectivos critérios, com três notas atribuídas conforme aspectos de proteção (protection), desempenho (performance) e usabilidade (usability), sendo a pontuação final a soma destes quatro, e dispostas na última coluna.

A organização define ainda os critérios para escolha dos melhores produtos, sendo aplicado aqueles que atingem a nota final máxima de 18 (dezoito) pontos.

A análise a seguir foi extraída do site da referida entidade, podendo ser aferida pelo link: **https://www.av-test.org/en/antivirus/business-windows-client/**, sendo este teste mais atual, sido realizado em dezembro de 2025 para a plataforma Windows 11. Foi feito um comparativo com 14 (quatorze) soluções de segurança para redes corporativas. A figura 1 abaixo demonstra os resultados dos testes conforme métrica estabelecida pela entidade:

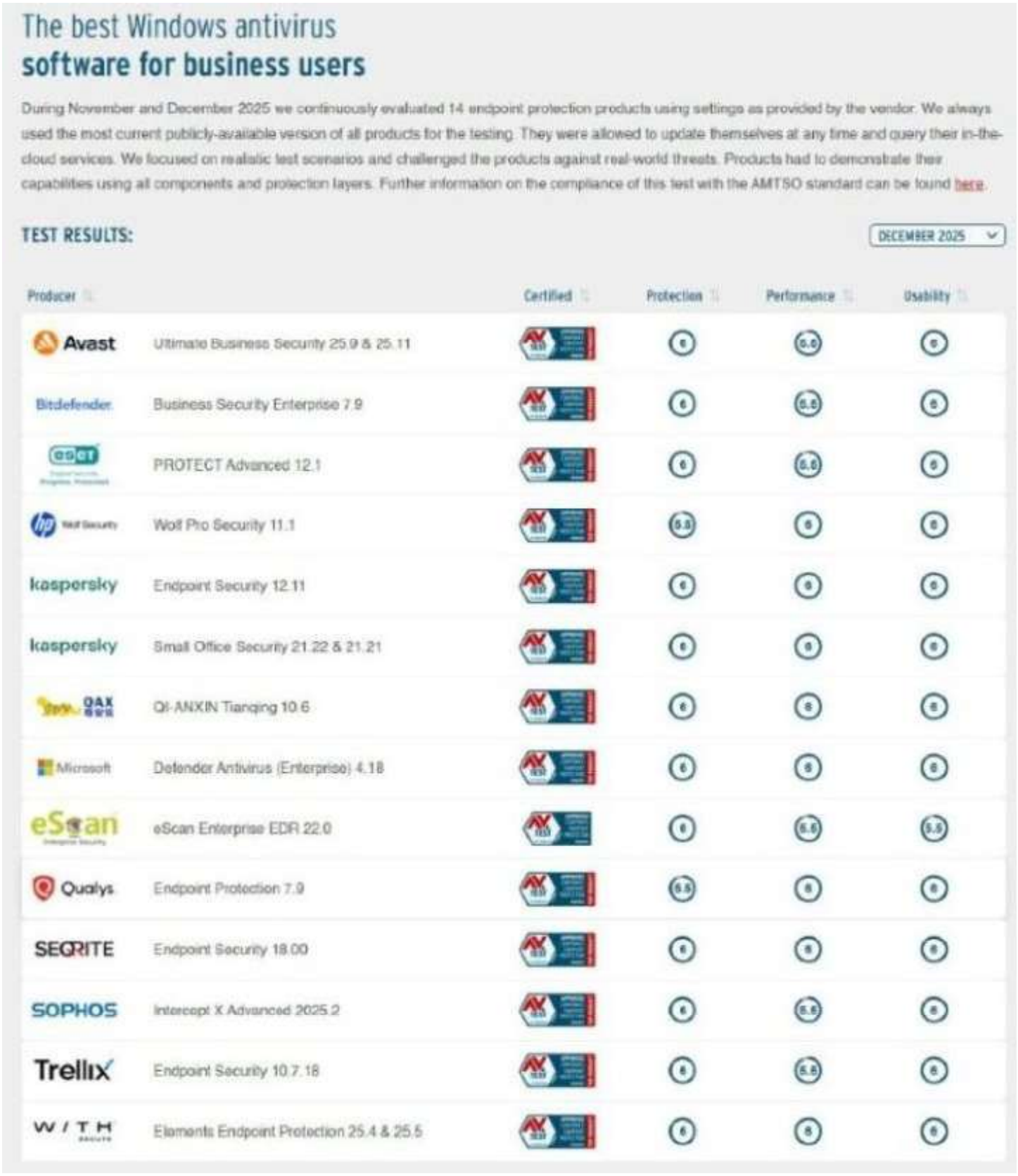

Figura 1 - Tabela comparativa de testes de soluções de antivírus corporativos.

Serão consideradas viáveis apenas as soluções que apresentaram nota acima de 17.5 pontos de um total de 18 pontos conforme ilustrado na tabela abaixo:

FABRICANTE	**PRODUTO**
Avast	Ultimate Business Security 25.9
Bitdefender	Business Security Enterprise 7.9
Eset	Protect Advanced 12.1

HP	Wolf Security 11.1
Kaspersky	Endpoint Security 12.11
Kaspersky	Small Office Security 21.22
Legendsec	QI-ANXIN Tianqing 10.6
Microsoft	Defender Antivirus (Enterprise) 4.18
Qualys	Endpoint Protection 7.9
Seqrite	Endpoint Security 18.00
Sophos	Intercept X Advanced 2025.2
Trellix	Endpoint Security 10.7.18
With	Elements Endpoint Protection 25.4 & 25.5

Sendo que a ESET PROTECT Advanced adquiriu nota 17.5 na avaliação do referido teste, e que este software já se encontra instalado nas cem maquinas que terão suas licença encerradas no dia 30 de junho de 2026, e o IGC necessita renovar ou realizar uma nova contratação para proteção e segurança do seu parque tecnológico, torna-se a escolha para a contratação/renovação da licença da ESET muito mais atrativa e vantajosa, por ser um software muito bem avaliado no quesito de proteção, desempenho e usabilidade, e sua renovação simplificaria todo o processo de execução operacional do sistema contratado.

10. Registro de soluções consideradas inviáveis

Para que a solução seja considerada viável para adoção no IGC, devem ser considerados os requisitos do item 5 -Necessidades Tecnológicas - deste documento, uma vez que os recursos descritos mencionam gerenciamento centralizado dos clientes em estações e servidores, bem como funcionamento em plataformas Windows e outros repositório central de atualizações e capacidade de armazenamento centralizado de eventos e geração de relatórios customizados.

Uma das soluções que não atende aos itens descritos é a solução Microsoft Windows Defender Antívirus. Ela é considerada inviável por não ser uma solução multiplataforma, ou seja, a mesma só funciona em sistemas operacionais Microsoft, mais precisamente em Windows 11.

Além disto, esta solução não dispõe de uma console de gerenciamento centralizado, conforme informado pela própria Microsoft, conforme texto disponível no link: https://docs.microsoft.com/pt-br/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security:

> "Embora o Windows Defender do Painel de Controle de Firewall possa proteger um único dispositivo em um ambiente doméstico, ele não fornece recursos de segurança ou gerenciamento centralizados suficientes para ajudar a proteger o tráfego de rede mais complexo encontrado em um ambiente empresarial típico."

Outras soluções que apresentem as mesmas características também devem ser consideradas inviáveis se não apresentarem os requisitos no item 5 deste documento. Ao considerar o Instituto AV-TEST como referência para a nossa análise técnica das soluções antivírus existentes no mercado, considerando seu relatório de análise mais recente, datado de dezembro de 2025, definimos o seguinte:

1- Serão descartadas soluções não testadas naquela oportunidade;

2 - Serão descartadas também as soluções com pontuação menor que 17.5 pontos na avaliação em questão.

11. Análise comparativa de custos (TCO)

Considerando que todas as soluções consideradas viáveis são softwares proprietários licenciáveis de mercado, o Custo Total de Propriedade será calculado de forma equivalente para todas as opções existentes. Desta forma não há o que se fazer em termos de análise comparativa de custos além do levantamento de estimativa do valor máximo admitido para a contratação.

12. Descrição da solução de TIC a ser contratada

1. Características Gerais da Solução

1.1. Deve possuir suporte nativo às arquiteturas 64-bits (x64) e ARM64, sendo o suporte a 32-bits desejável apenas para ambientes legados estritamente justificados;

1.2. Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho com no mínimo 4GB de memória RAM;

1.3. Deve suportar as seguintes plataformas Microsoft (clientes/desktops):

1.3.1. Windows 10 (versões com suporte ativo/LTSC), Windows 11 e superiores;

1.4. Deve suportar as seguintes plataformas Microsoft (servidores):

1.4.1. Windows Server 2022 e superiores;

1.4.2. Windows Server 2019 e superiores;

1.4.3. Desejável suporte ao Windows Server 2016 para ambientes legados justificados;

1.5. Deve inclusive suportar a instalação e operação em modo Server Core;

1.6. Deve suportar, pelo menos a função de proteção de endpoint (EPP/EDR), nas seguintes distribuições Linux com kernel moderno (Série 5.x ou superior):

1.6.1. Red Hat Enterprise Linux 8 e superiores, arquitetura 64-bits;

1.6.2. SUSE Linux Enterprise Server/Desktop 15 e superiores, arquitetura 64-bits;

1.6.3. Ubuntu Server/Desktop 20.04 LTS, 22.04 LTS, 24.04 LTS e superiores, arquitetura 64-bits;

1.6.4. Debian 11 e superiores, arquitetura 64-bits;

1.7. Deve suportar a instalação de agente e endpoint nos sistemas operacionais acima virtualizados nas seguintes plataformas de nuvem e hipervisores:

1.7.1. AWS (Amazon Web Services);

1.7.2. Microsoft Azure;

1.7.3. GCP (Google Cloud Platform);

1.7.4. Citrix Virtual Apps (XenApp);

1.7.5. Citrix Virtual Desktops (XenDesktop);

1.7.6. Citrix Hypervisor (XenServer);

1.7.7. Microsoft Hyper-V 2019 e superiores;

1.7.8. VMware ESXi (Versões 7.0, 8.0 e superiores);

1.7.9. VMware Player;

1.7.10. VMware vSphere;

1.7.11. VMware Workstation;

1.7.12. OpenStack.

1.8. Toda a proteção deverá ser realizada através de um único agente de proteção (Single Agent) com as funcionalidades descritas neste termo, não sendo aceitos plugins ou softwares adicionais na estação para a composição do pacote de segurança;

1.9. O agente único deve compreender, no mínimo, as seguintes funcionalidades:

1.9.1. Módulo antimalware de próxima geração (EPP);

1.9.2. Módulo de proteção contra ameaças avançadas (EDR/XDR);

1.9.3. Desejável módulo de proteção de dados (DLP Endpoint);

1.9.4. Desejável módulo para resposta a incidentes (isolamento de rede e remediação);

1.9.5. Desejável módulo de inteligência integrada contra ameaças (Threat Intelligence);

1.9.6. Módulo para controle de dispositivos removíveis (Device Control);

1.10. Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:

1.10.1. Relatórios dinâmicos;

1.10.2. Dashboards interativos;

1.10.3. Gestão de Políticas;

1.10.4. Configuração global;

1.10.5. Instalação e Desinstalação remota;

1.10.6. Integração com produtos de terceiros via API (ex.: SIEM/SOAR);

1.11. O cliente (agente) deve ser capaz de operar em modo autônomo (self-managed), aplicando políticas de contingência em caso de perda de comunicação com o servidor;

1.12. O cliente deve ser capaz de atualizar a telemetria para detecção de ameaças, seus patches e hotfixes a partir de um servidor definido pelo administrador ou diretamente na nuvem do fabricante;

1.13. A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise contextual mais inteligente (XDR);

1.14. A solução deve possuir múltiplas camadas de proteção (Machine Learning, Análise Comportamental, Inteligência Artificial e Heurística Avançada), não sendo aceitas soluções baseadas apenas em assinaturas estáticas;

1.15. A solução deve conter módulo capaz de proteger contra botnets, ataques de negação de serviço (DoS/DDoS), executáveis não confiáveis e conexões web maliciosas (Firewall local/NIDS);

1.16. A solução deve conter módulo web integrado capaz de garantir uma navegação segura, prevenindo contra sites de phishing, downloads de malwares e garantindo a aplicação de políticas de acesso (Permitir/Negar);

1.17. A plataforma deverá permitir automação de tarefas como: agendar varreduras (scans), envio de relatórios, atualizações, atribuição dinâmica de política por grupo e iniciar uma ativação de um agente;

1.18. É desejável que a solução de segurança para desktops e servidores possa se conectar a módulos de correlação e investigação reversa de incidentes na nuvem (Threat Hunting/Data Lake do fabricante).

2. Regras de Prevenção de Intrusão (HIPS) e Controle do Sistema

2.1. O módulo HIPS deve permitir controle granular e monitoramento sobre as seguintes ações:

2.2. Acesso remoto a pastas locais e compartilhamentos de rede;

2.3. Alteração de políticas de direitos das contas de usuários (UAC/IAM);

2.4. Alteração dos registros de extensão dos arquivos e associações de software;

2.5. Criação de novos arquivos em diretórios nativos do sistema, como Arquivos de Programas e AppData;

2.6. Criação de novos executáveis ou injeção de binários na pasta Windows (ex.: System32);

2.6. 1.Criar ou modificar remotamente arquivos do tipo Portable Executable (PE), scripts, variáveis de ambiente e localizações do sistema;

2.7. Criar ou modificar remotamente arquivos ou pastas sensíveis;

2.8. Tentativas de desativação ou bypass do editor de registro, gerenciador de tarefas e PowerShell;

2.9. Execução de arquivos a partir das pastas do usuário (ex.: Downloads, Temp);

2.10. Execução de scripts pelo Windows Script Host, PowerShell, Python ou interpretadores similares;

2.11. Instalar objetos auxiliares à navegação (BHOs), plugins ou extensões de shell;

2.12. Instalar e registrar novos CLSIDs, APPIDs e TYPE LIBs (objetos COM/DCOM);

2.13. Modificar configurações de rede de forma furtiva (ex.: DNS hijacking, rotas, proxy);

2.14. Modificar configurações de segurança dos navegadores web modernos (Edge, Chrome, Firefox);

2.15. Modificar processos principais do Windows, contemplando as seguintes ações:

2.15.1. Navegadores iniciando processos e programas não autorizados a partir da pasta de downloads;

2.15.2. Registrar programas para execução automática (chaves de Autostart/Run);

2.16. As regras especificadas na política do HIPS devem permitir o:

2.16.1. Bloqueio da ação, ou;

2.16.2. Geração de Evento de Informação (Auditoria/Log), ou;

2.16.3. Bloqueio e Geração de Evento de Informação simultaneamente;

2.17. A solução deve permitir ao administrador criar regras customizadas contendo, no mínimo, os seguintes parâmetros:

2.17.1. Processos:

2.17.1.1. Nome do processo;

2.17.1.2. Hash do arquivo (SHA-256 ou MD5);

2.17.1.3. Assinatura Digital/Certificado;

2.17.2. Usuário (integrado à base de identidades, ex.: AD);

2.17.3. Ações em Arquivos:

2.17.3.1. Criação;

2.17.3.2. Exclusão;

2.17.3.3. Execução;

2.17.3.4. Alteração de permissão;

2.17.3.5. Leitura;

2.17.3.6. Renomeação;

2.17.3.7. Escrita;

2.17.4. Chave de Registro:

2.17.4.1. Escrita;

2.17.4.2. Criação;

2.17.4.3. Exclusão;

2.17.4.4. Leitura;

2.17.4.5. Enumeração;

2.17.4.6. Carregamento;

2.17.4.7. Substituição;

2.17.4.8. Restauração;

2.17.5. Alterar permissão;

2.17.6. Valor de Registro:

2.17.6.1. Leitura;

2.17.6.2. Criação;

2.17.6.3. Exclusão;

2.17.7. Ações de Processo:

2.17.7.1. Qualquer acesso;

2.17.7.2. Criação de thread (injeção remota);

2.17.7.3. Modificação do payload;

2.17.7.4. Finalização (Tampering);

2.17.7.5. Execução;

2.18. A plataforma deve permitir a configuração de exclusões granulares de regras do HIPS.

3. Características da Varredura ao Acessar (Tempo Real / EPP)

3.1. A varredura residente deve ser passível de habilitação ou desativação por opção do administrador via console;

3.2. Deve iniciar a proteção na camada de driver durante a inicialização do sistema operacional (tecnologia ELAM - Early Launch Anti-Malware);

3.3. Deve ser capaz de realizar análise no setor de boot (incluindo UEFI e Secure Boot);

3.4. O administrador da solução deve poder especificar o tempo máximo de análise (timeout) para um único arquivo, evitando travamentos;

3.5. Deve analisar os processos em memória durante a inicialização do serviço e após a atualização da base de telemetria;

3.6. Deve possibilitar ao administrador a criação de bypass temporário ou análise otimizada para instaladores corporativos assinados e confiáveis;

3.7. Deve realizar inspeção ativa durante a cópia de arquivos entre pastas locais, unidades de rede e nuvem mapeada;

3.8. A solução deve possuir conexão ativa em tempo real com a Nuvem de Inteligência de Ameaças (Threat Intelligence) do fabricante, passível de ativação ou desativação por parte do administrador;

3.9. Deve permitir a configuração do nível de agressividade da análise heurística entre:

3.9.1. Muito Baixo;

3.9.2. Baixo;

3.9.3. Médio;

3.9.4. Alto;

3.9.5. Muito Alto;

3.10. Deve possibilitar aplicar as configurações de varredura a todos os processos do sistema operacional ou restringir a uma lista de grupos específica criada pelo administrador;

3.11. Deve realizar varredura de inspeção quando o processo realizar as seguintes ações de I/O:

3.11.1. Ler o disco;

3.11.2. Gravar no disco;

3.11.3. Deixar a solução decidir de forma automática baseada em inteligência;

3.12. Deve possibilitar análise nativa nos seguintes locais e formatos:

3.12.1. Unidades de Rede mapeadas (SMB/NFS);

3.12.2. Arquivos abertos para backup (suportando limites de performance para não impactar a rotina);

3.12.3. Arquivos compactados com algoritmos modernos, por exemplo .jar, .zip e outros;

3.12.4. Arquivos codificados e scripts embutidos (MIME, Base64);

3.13. Deve detectar Aplicações Potencialmente Indesejadas (PUA/PUPs), ameaças de dia zero (Zero-Day) em programas desconhecidos e ameaças embutidas em macros desconhecidas;

3.14. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação automática após detectar uma ameaça confirmada (malware):

3.14.1. Limpar o arquivo;

3.14.2. Excluir o arquivo;

3.14.3. Isolar ou Negar acesso ao arquivo;

3.15. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação automática após detectar um programa indesejado (PUA):

3.15.1. Limpar o arquivo;

3.15.2. Excluir o arquivo;

3.15.3. Permitir acesso ao arquivo (via aprovação);

3.15.4. Negar acesso ao arquivo;

3.16. Deve possibilitar ao administrador a gestão centralizada de uma lista de exclusões confiáveis (por caminho, hash ou certificado);

3.17. Deve possuir integração com recursos do sistema (ex.: AMSI) capazes de interceptar e analisar scripts ofuscados na memória (Javascript, VBScript, PowerShell) indicando se o comportamento é malicioso ou não;

3.18. Deve permitir a criação de listas de exclusão de URLs confiáveis que não sofrerão interceptação rígida e análise de scripts;

3.19. Ao detectar uma ameaça, o agente deverá emitir uma notificação nativa no sistema operacional ao usuário com uma mensagem customizável pelo administrador da solução.

4. Características Varredura Sob Demanda

4.1. Deve ser possível realizar varreduras agendadas com periodicidade diária, semanal ou customizada;

4.2. Deve permitir a criação de repetição da tarefa na console;

4.3. Deve permitir definir a hora exata da execução da tarefa de análise;

4.4. Deve permitir a criação da tarefa de varredura com janela aleatória (randômica) para evitar sobrecarga de I/O em ambientes de virtualização simultâneos;

4.5. Deve permitir a realização de varreduras agendadas apenas após o logon do usuário ou durante a inicialização do sistema operacional;

4.6. Deve permitir ao administrador escolher (um ou mais) alvos granulares da varredura, dentre eles:

4.6.1. Os locais da varredura contemplando:

4.6.1.1. Memória RAM (para detecção de rootkits e malwares fileless);

4.6.1.2. Processos em execução;

4.6.1.3. Arquivos e chaves do Registro do sistema;

4.6.1.4. "Meu Computador" ou "Este Computador";

4.6.1.5. Todas as unidades locais do disco;

4.6.1.6. Todas as unidades de armazenamento fixas;

4.6.1.7. Todas as unidades de armazenamento removíveis;

4.6.1.8. Todas as unidades mapeadas na rede;

4.6.1.9. Pasta inicial/Boot;

4.6.1.10. Pastas de perfil do usuário (ex.: AppData, Downloads);

4.6.1.11. Pasta base do Windows;

4.6.1.12. Pasta de Arquivos de Programas;

4.6.1.13. Pasta de arquivos temporários do sistema;

4.6.1.14. Lixeira do sistema operacional;

4.6.1.15. Qualquer arquivo ou pasta específica delimitada pelo administrador;

4.6.1.16. Setor de inicialização física/lógica (boot/UEFI);

4.6.1.17. Arquivos compactados em sua totalidade;

4.6.1.18. Arquivos estruturados em MIME;

4.6.2. Os tipos de arquivos específicos que serão analisados por extensão ou cabeçalho;

4.6.3. Opções adicionais de detecção durante o scan, como detecção de programas indesejados (PUA), ameaças de dia zero e macros maliciosas;

4.6.4. Áreas de exclusão específicas que não deverão ser varridas sob hipótese alguma para garantir compatibilidade com sistemas internos críticos;

4.7. Deve permitir a integração direta com o Centro de Inteligência na Nuvem do fabricante durante a varredura agendada para validação de falsos positivos;

4.8. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça confirmada na varredura sob demanda:

4.8.1. Limpar o arquivo infectado;

4.8.2. Excluir o arquivo malicioso;

4.8.3. Negar acesso/Isolar o arquivo em quarentena;

4.9. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado (PUA):

4.9.1. Limpar o arquivo;

4.9.2. Excluir o arquivo;

4.9.3. Permitir acesso mediante aprovação de política;

4.9.4. Negar acesso ao arquivo;

4.10. Para minimizar o impacto sistêmico e no trabalho do usuário final, a solução deve permitir tecnologias de otimização contendo:

4.10.1. Utilização de cache inteligente (Smart Cache), ou seja, arquivos já analisados que não tiveram seu conteúdo e hash alterados não serão reprocessados;

4.10.2. Capacidade de iniciar a varredura apenas e tão somente quando o sistema operacional estiver em estado de ociosidade (idle);

4.10.3. Permitir ao usuário ou administrador pausar e retomar varreduras manualmente;

4.11. Deve permitir ao administrador inserir uma conta de serviço de domínio via console para realizar a análise em dispositivos de armazenamento de rede (NAS/Storages) de forma autenticada.

5. Características do Módulo de Ameaças Avançadas (EDR/XDR e Ransomware)

5.1. A solução deve possuir tecnologia de isolamento ou confinamento dinâmico (Sandboxing local ou em nuvem) de aplicativos e arquivos executáveis com comportamentos suspeitos, como tentativas de criptografia (ransomware);

5.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente micro-virtualizado ou emulado controlado antes de permitir a execução real no sistema;

5.3. Deve permitir a indicação de aplicações confiáveis em lista de permissões para que sistemas internos não caiam no filtro de confinamento dinâmico (falsos positivos);

5.4. A proteção anti-ransomware de análise comportamental não deve requerer obrigatoriamente conexão com a internet ou centro de inteligência para que a contenção da ameaça seja ativada;

5.5. A solução deve manter um cache de reputação local com informações de aplicações dinamicamente categorizadas (conhecidas, desconhecidas e maliciosas);

5.6. Dentre os Comportamentos Indicadores de Ataque (IoAs) monitorados e passíveis de prevenção, a solução deve ser capaz de:

5.6.1. Bloquear acesso local a partir de cookies maliciosos;

5.6.2. Bloquear a criação massiva de arquivos a partir de extensões de risco automatizado como .bat, .exe, .html, .hpg, .jpg, .bmp, .job e scripts . vbs / .ps1;

5.6.3. Bloquear a criação não autorizada de arquivos executáveis em qualquer local mapeado na rede;

5.6.4. Bloquear a criação ou manipulação de CLSIDs, APPIDs e TYPELIBs usados em ataques fileless;

5.6.5. Bloquear injeções e criação de threads remotas em outros processos legítimos do sistema (ex.: Process Hollowing);

5.6.6. Bloquear a tentativa de desativação de executáveis ou serviços críticos do sistema operacional ou da própria solução antivírus (Tamper Protection);

5.6.7. Bloquear a leitura, exclusão ou gravação atípica em lote de arquivos estruturados frequentemente visados por ransomwares (documentos, planilhas, bancos de dados);

5.6.8. Bloquear a gravação clandestina ou extração de leitura na memória de processos críticos alheios (ex.: proteção ao LSASS para evitar roubo de credenciais);

5.6.9. Bloqueio de modificação indevida das políticas do Firewall nativo do Windows;

5.6.10. Bloqueio de modificação anômala ou adição de malwares na pasta de tarefas agendadas do Windows;

5.6.11. Bloqueio de modificação de arquivos vitais de inicialização do Windows e locais críticos do Registro do sistema;

5.6.12. Bloqueio de modificação parasitária em arquivos executáveis portáteis (PE) já compilados;

5.6.13. Bloqueio de manipulação do bit de atributo oculto (hidden) em diretórios de sistema;

5.6.14. Bloqueio de manipulação forçada do bit de atributo somente leitura em arquivos de proteção;

5.6.15. Bloqueio de modificação de entradas de registro sensíveis como DLL AppInit;

5.6.16. Bloqueio de modificação de chaves e locais do Registro responsáveis pela inicialização do SO;

5.6.17. Bloqueio de modificação em lote ou exclusão de pastas de dados nativas de usuários;

5.6.18. Bloqueio de modificação ou sequestro do local do Registro de Serviços do sistema;

5.6.19. Bloqueio de suspensão indevida ou travamento de processos cruciais;

5.6.20. Bloqueio de término ou finalização violenta de processos críticos do sistema;

5.7. A partir dos comportamentos maliciosos observados, deve ser possível à solução aplicar ação de bloqueio automático da ameaça ou gerar apenas evento de informação (modo de auditoria), conforme política configurada;

5.8. Deve ser capaz de informar ao usuário final, caso configurado, os comportamentos de risco e ameaças bloqueadas através de notificação pop-up com mensagem customizada;

5.9. Deve possuir o modo de ativação de bloqueio proativo para o confinamento de quaisquer arquivos desconhecidos (Zero-Day) acessados pelo sistema operacional e não possuidores de reputação global;

5.10. O administrador deve poder atribuir perfis de regras baseados no equilíbrio estratégico da política, visando aplicar maior rigidez de segurança ou maior flexibilidade para a produtividade do usuário final;

5.11. Toda a proteção de detecção avançada (EDR) deve estar nativamente embutida no mesmo agente de proteção (Single Agent), não requerendo download secundário, sensor separado ou aplicação adicional na estação de trabalho para a execução e ativação do monitoramento;

5.12. Deve possuir capacidade de inspecionar arquivos suspeitos, correlacionar eventos e detectar anomalias comportamentais utilizando técnicas nativas de Inteligência Artificial e "Machine-Learning" sem depender primariamente de vacinas/assinaturas legadas.

6. Módulo para Controle de Dispositivos Removíveis (Device Control / DLP)

6.1. Deve controlar ativamente o modo como os usuários copiam ou acessam dados em drives USB, cartões de memória, mídias óticas e magnéticas, dispositivos Bluetooth e IrDA, dispositivos de leitura de imagem (MTP), smartphones, portas legadas (COM/LPT) ou interfaces modernas (Thunderbolt /USB-C);

6.2. Deve permitir que o administrador especifique granuralmente quais dispositivos podem ou não ser usados utilizando parâmetros de hardware, incluindo: códigos do produto (PID), códigos de fornecedor (VID), números de série exclusivos do pendrive/disco, classes de dispositivos ou identificadores de nome;

6.3. O módulo deve ser capaz de coletar dados contextuais de incidentes tais como identificação do dispositivo, data/hora da inserção, usuário logado e evidências das ações de leitura/gravação, exportando as métricas para reação, investigação e auditoria na console central;

6.4. Deve permitir a aplicação de regras de reação específicas para unidades de mídia removível (ex.: pendrive) com opções mandatórias de: bloqueio total de acesso, acesso em modo somente leitura (read-only) ou acesso total com monitoramento e gravação de logs (auditoria);

6.5. Deve ser capaz de monitorar automaticamente o uso das interfaces listadas e aplicar o bloqueio de todas as tentativas de uso e evasão de política em tempo real;

6.6. Deve possuir integração nativa com a ferramenta de gerenciamento centralizado para o envio e coleta de logs essenciais para o cumprimento de normativas de privacidade (ex.: LGPD), contendo device, timestamp e metadados da transação;

6.7. Deve suportar integração direta com a estrutura de identidades corporativas (Active Directory / Entra ID) para a criação e amarração de regras de acesso a dispositivos baseadas em usuários, grupos de domínio ou Unidades Organizacionais (OUs);

6.8. Deve bloquear de forma nativa a tentativa do usuário de desabilitar o serviço, modificar os processos ou desinstalar o agente de proteção da estação de trabalho (Tamper Protection), permitindo a remoção apenas mediante inserção de senha de desinstalação configurada e fornecida pelo administrador central.

7. Características do Módulo de Gerenciamento Centralizado

7.1. A ferramenta de console de gerenciamento local (se instalada On-Premise) deve suportar a instalação em ambientes virtualizados contendo os seguintes sistemas operacionais base:

7.1.1. Windows Server 2025 e Windows Server 2022;

7.1.2. Windows Server 2019;

7.1.3. Desejável suporte de estabilidade ao Windows Server 2016 caso exigido por restrições de arquitetura de legado interno;

(Itens antigos referentes a Windows 2008 R2 e 2012 foram descontinuados no escopo de instalação segura de consoles de segurança, devendo a numeração ser atendida pelo fornecimento das instâncias atualizadas);

7.1.4. É desejável e plenamente aceito o fornecimento opcional de um Virtual Appliance (Appliance virtual no formato OVA/OVF) por parte da contratada, contendo uma distribuição Linux embarcada e segura para implantação rápida (Plug-and-Play) da console em hypervisors compatíveis com os requisitos deste ETP;

7.2. A arquitetura exigida para a instalação da console de gerenciamento ou servidor de aplicação deve ser exclusivamente de 64-bits;

7.3. O módulo de banco de dados e gerenciamento deve suportar ser implantado de forma redundante em cluster Microsoft (High Availability);

7.4. Toda a camada de comunicação do gerenciamento deve possuir suporte nativo e pleno aos protocolos de rede IPv4 e IPv6 (Dual-Stack);

7.5. Deve suportar implantação e operação 100% suportada em sistemas operacionais devidamente virtualizados ou hospedados na nuvem (IaaS);

7.6. Para o armazenamento da inteligência e telemetria, deve possuir suporte a bases de dados estruturadas:

7.6.1. Microsoft SQL Server 2019 ou edições superiores;

7.6.2. Desejável suporte a instâncias modernas de MySQL (versões 8.0 ou superiores, 64 bits);

7.6.3. Desejável suporte a PostgreSQL e MariaDB modernos em arquitetura 64 bits para maior flexibilidade arquitetural;

7.7. Toda a interface de administração da console de gerência deve possuir acesso exclusivamente via WEB, unificando a experiência no modelo "Single Pane of Glass";

7.8. A interface web gerencial deve ser nativamente compatível com os seguintes navegadores corporativos padrão:

7.8.1. Google Chrome e navegadores baseados no motor Chromium;

7.8.2. Mozilla Firefox;

7.8.3. Apple Safari nas suas edições com suporte ativo;

7.8.4. Microsoft Edge;

7.9. Em implantações On-Premise de larga escala, deve ser possível segregar a arquitetura de instalação dos componentes da solução de gerência em servidores distintos:

7.9.1. Servidor responsável pela interface da Console Web;

7.9.2. Servidor de hospedagem da Base de Dados;

7.9.3. Servidor de comunicação, telemetria e gerenciamento de endpoints (Proxy/Relay de interação);

7.9.4. Agentes na rede configurados como distribuidores de atualizações locais de vacina/cache para economia de link de internet;

7.10. O banco de dados da aplicação deve suportar o uso nativo de instâncias SQL Server rodando sob volumes lógicos em Storage Area Networks (SAN);

7.11. Deve permitir a configuração e a geração automatizada dos instaladores (agentes) para todos os módulos da solução a partir de um único console;

7.12. Deve permitir a propagação e a alteração instantânea das configurações dos módulos nos clientes (endpoints) de maneira remota, silenciosa e sem exigir reinicialização massiva;

7.13. Deve possuir a capacidade de integração do gerenciamento de estações de trabalho e de servidores deste mesmo fabricante, a fim de prover uma única e universal console de gerenciamento centralizado de todas as soluções de segurança de endpoint (single agent/single console);

7.13.1. O sistema de distribuição deve permitir a atualização de forma estritamente incremental das bases de inteligência e vacinas nos clientes finais, a partir de um único servidor ou proxy local, reduzindo drasticamente o consumo de banda WAN corporativa;

7.14. A console deve extrair e permitir a visualização em formato de inventário básico das características de hardware (CPU, RAM, Disco) e software dos endpoints gerenciados;

7.15. Deve permitir integração, leitura e sincronização bidirecional automática com a árvore hierárquica e grupos de segurança de domínios Microsoft Active Directory (AD) ou Microsoft Entra ID existentes na rede local;

7.16. Deve permitir a criação centralizada de tarefas em lote (Deployment Tasks) para atualização de versão de motor de agentes, varreduras programadas e upgrades de inteligência programados para execução imediata, periódica, ou ativada no momento da inicialização / logon da estação na rede;

7.17. Deve reter e permitir a auditoria das informações coletadas dos endpoints armazenando logs, eventos e políticas de bloqueio de maneira durável no banco de dados centralizado;

7.18. Deve garantir governança administrativa suportando controle de acesso baseado em funções (RBAC), permitindo a criação de diferentes níveis de administração da console, com perfis customizáveis de maneira independente ou associados ao login da rede do administrador (SSO);

7.19. O sistema de gestão de privilégios deve contemplar múltiplos administradores com acesso restrito focado a grupos operacionais distintos (ex.: administrador com visão de filiais, operador somente leitura) a fim de respeitar as permissões de acesso aos produtos gerenciados;

7.20. Deve permitir a construção e gestão de agrupamentos dinâmicos de endpoints com base em regras estáticas como faixas e blocos de número IP/Sub-redes associadas ao cliente;

7.21. Deve permitir a classificação avançada na rede através da criação de grupos virtuais baseados em "Marcadores" dinâmicos (Tags);

7.22. O sistema de regras lógicas deve permitir que a console posicione o endpoint automaticamente dentro de grupos hierárquicos ao ler os seguintes critérios dinâmicos da máquina: tipo de sistema operacional, módulos instalados, tempo da última conexão, risco e vulnerabilidade detectada, dentre outros;

7.23. A comunicação arquitetural deve forçar proativamente (modo de enforcement) que as políticas e senhas parametrizadas no servidor cheguem e sejam acatadas imperativamente pelos endpoints conectados;

7.24. Como mecanismo de resiliência, caso um usuário local altere a configuração por vias excepcionais, a mesma deverá ser sobrescrita automaticamente, retornando ao padrão estabelecido na política oficial do servidor de gerência assim que o agente se comunicar;

7.25. Para a garantia do sigilo, a comunicação de dados, de comandos executivos e as atualizações de inteligência trocadas entre os agentes na ponta e o servidor de gerenciamento deve transitar de forma segura e criptografada (ponta-a-ponta) utilizando protocolos TLS modernos via HTTPS (mínimo exigido TLS 1.2);

7.26. Deve fornecer suporte a tarefas mandatórias para forçar a remediação e a instalação faltante dos módulos requeridos nos clientes não conformes;

7.27. O serviço no agente deve ser autorreparável. Caso ocorra uma desinstalação acidental ou maliciosa, o processo guardião ou as tarefas da gerência devem prover o reparo automático e reinstalação imediata;

7.28. O instalador gerado pela plataforma de gerenciamento deverá possuir tecnologia embarcada capaz de forçar de forma desassistida (silenciosa) a desinstalação e a remoção de chaves de registro residuais de produtos de antivírus concorrentes, EDRs, agentes desatualizados ou soluções legadas que já operem nas estações para evitar conflitos de software na implantação;

7.29. A central administrativa do módulo de gestão deverá consolidar, relatar e orquestrar nativamente, no mínimo, as seguintes soluções do escopo:

7.29.1. O módulo gerencial da solução voltada para proteção antimalware e heurística em estações de trabalho e sistemas de servidores (EPP);

7.29.2. O módulo gerencial da funcionalidade avançada responsável pela correlação e resposta a incidentes sofisticados, como análise forense comportamental e detecção contínua na estação (EDR/XDR);

7.29.3. O módulo de regras estritas exigidas para proteção nativa do workload de servidores críticos de rede;

7.29.4. A plataforma deve dispor de um motor de relatórios em formato gráfico, possibilitando a criação de templates, consultas customizáveis e personalização visual detalhada na geração de reportes estatísticos e executivos;

7.29.5. Os relatórios analíticos extraídos a partir da plataforma deverão possuir funcionalidade para exportação ou agendamento de envio automático via e-mail utilizando obrigatoriamente os padrões de arquivo do mercado, incluindo: HTML, CSV, PDF e XML;

7.29.6. O motor de governança e compliance do gerenciador deverá fornecer consultas e relatórios imediatos contendo um detalhamento minucioso do status do ambiente, informando:

7.29.6.1. O levantamento estatístico integral evidenciando os endpoints (máquinas) cuja lista de definições locais da vacina/agente encontre-se em estado de atraso ou defasagem perante o servidor central;

7.29.6.2. O catálogo detalhado com controle de conformidade, extraindo a build de versão de software ou agente, incluindo as telemetrias com apoio na nuvem do fabricante ativas naquele exato momento em cada endpoint pesquisado;

7.29.6.3. A catalogação gráfica e de volumetria informando, por assinatura ou categoria (MITRE ATT&CK), os vetores de vírus, malwares e PUPs/PUAs identificados com maior reincidência global de tentativas de ataque à infraestrutura da rede;

7.29.6.4. Os relatórios investigativos evidenciando de forma nominal (nome de host ou IP) as estações de trabalho mapeadas como alvo preferencial e que mais registraram interações de logs focados em mitigação de infecção em um escopo ou janela de dias previamente definida na busca;

7.29.6.5. Os relatórios extraídos correlacionando identidades e destacando com ênfase as contas de perfis de usuário logadas nos instantes críticos onde o agente mais detectou comportamentos suspeitos e evitou comprometimentos ativos contra a rede corporativa, suportando filtro por um período parametrizado;

7.29.7. Possibilidade unificada de licenciamento, ativação, delegação e administração tática para que a equipe técnica utilize todos os módulos integrantes da suíte a partir desta tela mestre (master pane);

7.29.8. O servidor e seus componentes web front-end não deverão depender apenas de linhas de base textual, provendo uma visualização moderna orientada a módulos gráficos ou minipainéis conhecidos como Dashboards na página inicial de acompanhamento (Home Screen);

7.29.9. Os módulos e visões gráficas presentes nos referidos Dashboards devem apresentar nativamente recursos interativos (clicáveis com técnica Drill-Down) de leitura prática, devendo o fornecedor assegurar a abrangência visual para todos os relatórios estratégicos mapeados anteriormente;

7.29.10. Possuir regras lógicas automáticas embutidas ou perfis móveis flexíveis na gerência central aptos a orientarem e manterem a atualização fluida para a proteção completa dos agentes de antivírus hospedados em equipamentos móveis e computadores em constante viagem, conhecidos como endpoints portáteis (como notebooks da força de vendas corporativa ou regime home office), realizando os devidos downloads em plano de fundo quer se encontrem acoplados presencialmente através de comunicação LAN via rede interna ou operando remotamente ancorados por túnel VPN;

7.29.11. Os fluxos lógicos voltados à redução de contenção de roteamento na distribuição na rede matriz ou filiais devem englobar a arquitetura provendo permissão ao uso orquestrado e simultâneo de inúmeros espelhos, também conhecidos com a denominação técnica de múltiplos repositórios internos locais, aptos a hospedarem fisicamente o volume de instalação matriz para as builds de novos produtos requisitadas via rede local, e a prover o espelhamento diário contendo os fragmentos de arquivo referenciando a vacina e assinaturas via mecanismo seletivo de sincronização diferencial entre tais servidores locais;

7.29.12. Para suprir de forma robusta e rastreável eventuais necessidades periciais da própria gerência de redes (certificações SOX e afins), deter no motor de registros uma base relacional sólida dispondo de capacidade técnica autônoma com retenção configurável para processar e exportar ininterruptamente históricos estruturados, registrando de forma inalterável a tabela de alterações nas normas de sistema bem como na atribuição de privilégios entre técnicos da empresa, popularmente chamada de registros/logs transacionais voltados à rotina de auditoria sistêmica e investigativa;

7.29.13. Na gestão macro dos milhares de endpoints operacionais mapeados na rede ou isolados via política autônoma, permitir dentro de sua base estrutural do gerenciamento a criação e associação múltipla atribuindo etiquetas lógicas personalizáveis ou tags predefinidas diretamente associadas ao inventário das máquinas virtuais ou computadores físicos registrados no banco, de modo a instrumentalizar este recurso permitindo ao próprio administrador usar estas tags como balizadores lógicos aptos a promover o cálculo do filtro condicional de movimentação e a distribuição autônoma de nós (equipamentos) reajustando-os e arrastando suas permissões por dentro dos subgrupos lógicos hierárquicos vigentes no coração da arquitetura desenhada em sua estrutura matricial de gerenciamento corporativo diário;

7.29.14. Conforme já estipulado no quesito central em itens supramencionados de especificação técnica e de comunicação de infraestrutura e serviços (Item 2.7.7), ser capaz de suportar por via nativa do fornecedor oficial a disponibilidade absoluta aos perfis sistêmicos exigindo que

todo seu leque interativo para configuração de chaves gerenciais seja suportado universalmente fornecendo amplo acesso interativo em sua interface ou à sua tela primária de console mestre conectando-se sob rigorosa exigência exclusivamente a interações web a partir de qualquer segmento validado e seguro (interface web-based SaaS e navegação).

13. Estimativa de custo total da contratação

Valor (R$): 22.930,56

A presente contratação esta com o valor total estimado de R$22.930,56 (Vinte e dois mil, novecentos e trinta reais e cinquenta e seis centavos). Conforme média dos valores apurados na pesquisa direta de preços e no painel de preços do governo federal, conforme consta nos autos do processo.

14. Justificativa técnica da escolha da solução

Visando a manutenção dos níveis desejáveis de segurança na operação das soluções TIC no âmbito do Instituto de Geociências, considerando que o IGC também aloca o datacenter que provê os sistemas críticos que viabilizam todas as atividades administrativas e acadêmicas do instituto, torna-se de importância vital a utilização de uma solução adequada, baseada nas boas práticas de mercado, como um software antivírus de nível corporativo, avaliado por instituições independentes dedicadas à analise específica destas soluções, que disponha de todas as funcionalidades necessárias para o controle efetivo de ataques que possam degradar os sistemas e/ou as informações neles contidos. Essa solução irá estabelecer uma barreira inicial contra tentativas de intrusão com objetivos como: extorsão mediante sequestro de informações, uso indevido de recursos de TIC, negação de serviços e outros que ocasionem solução de continuidade das atividades laborais do IGC de forma parcial ou plena, com consequências incalculáveis. Com todo o parque de equipamentos sendo monitorado em tempo real, a gestão centralizada da segurança, relatórios de situação, etc, o Setor de TI conseguirá cumprir sua missão principal que é a de manter os recursos de TIC disponíveis a todos os colaboradores, dentro dos melhores padrões operacionais existentes.

15. Justificativa econômica da escolha da solução

Considerando que a falta da solução em questão permitirá a ocorrência de eventos catastróficos com impactos negativos incalculáveis para o Instituto de Geociências, a renovação do antivírus ESET já se caracteriza justificável do ponto de vista econômico já que trará redução de custos imprevistos com mitigação de riscos. Outro fato é que a solução pretendida já está devidamente consagrada no Instituto como melhor alternativa de mercado para as demandas existentes, justificando-se economicamente também pela possível disputa entre os prováveis fornecedores que poderão participar do certame com perspectiva de redução dos valores de referência e consequente economia para a administração.

16. Benefícios a serem alcançados com a contratação

- Manutenção dos níveis de segurança da informação desejáveis para as atividades orgânicas do Instituto de Geociências, de forma ininterrupta e dentro do que preconizam as boas práticas de mercado.
- Continuidade dos serviços críticos de segurança da informação;
- Redução de vulnerabilidades e riscos cibernéticos;
- Consolidação da governança de TIC.

17. Providências a serem Adotadas

Devido a possibilidade de renovação do software antivírus, o processo torna-se simplificado na questão operacional. Não ocasionando novas demandas para o Setor de Tecnologia da Informação da Unidade, que providenciará a instalação de todas as licenças com suas respectivas quantidades de usuários do software ESET nas maquinas (desktop) do Laboratório e dos setores administrativos que serão contemplados pelo antivírus no Instituto de Geociências/UFMG.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

A comissão constituída pela Portaria Nº 5244 de 03/06/2026, em atendimento a Instrução Normativa nº 1 de 04/04/2019, responsável pela elaboração deste Estudo Técnico Preliminar evidenciou que a contratação do software aqui descrito, mostra-se possível em sua forma técnica e fundamental para o atendimento às necessidades administrativas, de ensino e pesquisa do Instituto de Geociências. Diante do exposto, declara-se ser viável a contratação pretendida.

19. 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.

GABRIEL AMARAL DE PINHO

Membro da comissão de contratação

Assinou eletronicamente em 18/06/2026 às 10:20:27.

VINICIUS ETRUSCO MOREIRA

Membro da comissão de contratação

Assinou eletronicamente em 18/06/2026 às 10:24:13.

BRUNO WILLIAM MENDES SALUSTIANO

Membro da comissão de contratação

Assinou eletronicamente em 18/06/2026 às 10:25:39.