ESTUDO TÉCNICO PRELIMINAR

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação. É o documento que descreve as análises realizadas em relação às condições da contratação em termos de necessidades, requisitos, alternativas, escolhas, resultados pretendidos e demais características, e que demonstra a viabilidade técnica e econômica da contratação.

CAPÍTULO 1: ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1. Contextualização

Contratação de empresa para aquisição de licença da solução de antivírus Kaspersky Next EDR Optimum com gerenciamento, para restabelecer a proteção cibernética das estações de trabalho, servidores e demais dispositivos de rede do Tribunal de Justiça Militar do Estado do Rio Grande do Sul (TJM/RS), atualmente expostos a vulnerabilidades devido à ausência de um software antivírus ativo. A solução atenderá às necessidades das unidades do Tribunal, incluindo a 1ª, 2ª Auditorias Militares, Santa Maria e Passo Fundo, garantindo a continuidade dos serviços jurisdicionais e administrativos com segurança e eficiência.

1.2. Identificação da demanda no Plano de Contratações de STIC

A contratação está conforme a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), instituída pela Resolução CNJ n.º 370/2021. A ENTIC-JUD visa promover a governança ágil e a transformação digital do Poder Judiciário, por meio de serviços e soluções digitais inovadoras que impulsionem sua evolução tecnológica. É importante ressaltar que esta contratação está alinhada aos Objetivos Estratégicos, letra c), Processos Internos:, Objetivo 6 Aprimorar as Aquisições e Contratações e Objetivo 8: Promover Serviços de Infraestrutura e Soluções Corporativas da ENTIC-JUD, contribuindo para a realização desses objetivos e para a aderência do órgão à Estratégia.

1.2.1. Alinhamento da Solução

No que tange ao Planejamento Estratégico do TJMRS, vislumbra-se o alinhamento aos objetivos estratégicos:

- 3: Aperfeiçoar a governança e a gestão de TIC;

- 4: Aprimorar as contratações;

- 5: Garantir e aperfeiçoar a infraestrutura de TIC necessárias às atividades administrativas e judicias.

No que concerne ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), para os anos de 20024/2025, Portaria n.º 127/2023-TJMRS, esta contratação atinge ações 1,5 e 6 do Plano de Ações: Processos Internos.

Esta contratação também será orientada, no que couber, as orientações e disposições contidas na Lei Geral de Proteção de Dados Pessoais, Lei n. 13.709, de 14 de agosto de 2018.

1.3. Caracterização da demanda

1.3.1. Definição e Especificação das Necessidades

A contratação tem por objetivo a aquisição de licença da solução de antivírus Kaspersky Next EDR Optimum com gerenciamento, e restabelecer a proteção cibernética das estações de trabalho, servidores e demais dispositivos de rede do Tribunal de Justiça Militar do Estado do Rio Grande do Sul (TJM/RS), atualmente expostos a vulnerabilidades devido à ausência de um software antivírus ativo. A solução atenderá às necessidades das unidades do Tribunal, incluindo a 1ª, 2ª Auditorias Militares, Santa Maria e Passo Fundo, garantindo a continuidade dos serviços jurisdicionais e administrativos com segurança e eficiência. Há possibilidade, uma vez que a demanda se

enquadra na categoria de serviços comuns, que trata a Lei nº 14.233/2021, por possuir padrões de desempenho e características gerais e específicas encontrada no mercado. O prazo da contratação será de 36 (trinta e seis) meses, podendo ser renovado por períodos sucessivos, conforme previsto na lei, até atingir o limite.

1.3.2 Definição e Especificação dos Requisitos

A contratação desta solução é imprescindível para assegurar a proteção robusta do ambiente computacional do TJM-RS, atendendo aos mais elevados padrões de segurança cibernética e garantindo a continuidade e eficiência das operações da Justiça Militar.

A solução de proteção contra vírus e outras ameaças cibernéticas é fundamental para garantir a segurança e a integridade do ambiente computacional do Tribunal de Justiça Militar do Estado do Rio Grande do Sul (TJM-RS). Para tanto, a contratação deve atender aos seguintes requisitos:

1.3.3. Requisitos Funcionais:

Com base na experiência pretérita e nas boas práticas do mercado, os requisitos funcionais para uma nova contratação devem considerar:

1.3.3.1 Definição dos Requisitos da Arquitetura Tecnológica (configuração)

1. Proteção Abrangente: A solução deve ser capaz de detectar, prevenir e eliminar uma ampla gama de ameaças cibernéticas, incluindo vírus, trojans, worms, ransomware e outras formas de malware;

2. Suporte Técnico Especializado: O fornecedor deve oferecer suporte técnico especializado, disponível para auxiliar na resolução de problemas, manutenção preventiva e atualizações. O suporte deve estar disponível em regime 24/7 para garantir a prontidão na resposta a incidentes críticos.

3. Direito de Uso e Licenciamento: A contratação deve incluir o direito de uso da solução de software por um período contínuo de 36 (trinta e seis) meses. O licenciamento deve abranger todas as estações de trabalho, servidores e notebooks utilizados pelo TJM-RS, garantindo conformidade com as políticas de uso de software;

4. Atualizações e Manutenções, a solução deve incluir atualizações regulares de versões, garantindo que o software permaneça atualizado com as últimas definições de vírus e melhorias de segurança. Isso inclui patches de segurança, upgrades de versões e quaisquer outras atualizações necessárias para manter a solução eficaz contra novas ameaças;

5. Integração e Compatibilidade: A solução deve ser compatível com a infraestrutura existente do TJM-RS, integrando-se perfeitamente com os sistemas e serviços de Tecnologia da Informação e Comunicação (TIC) já em uso. Isso inclui compatibilidade com sistemas operacionais, plataformas de rede e outros softwares de segurança;

- Sistemas Operacionais em Uso e Versões: Atualmente, utilizamos Windows 10 e Windows 11 em estações de trabalho, 1x Windows Storage Server 2016 Standard e 2x Windows Server 2012 R2 Standard.

- Versão do Sistema Operacional dos Servidores Físicos: Os servidores físicos utilizam 1x Windows Storage Server 2016 Standard e 2x Windows Server 2012 R2 Standard

- O TJMRS possui Active Directory (AD) implementado. Um firewall corporativo em uso. A solução adotada atualmente é FortiGate.

- O ambiente conta com conexão dedicada de alta disponibilidade.

- Atualmente, a velocidade contratada é de 100 Mbps com redundância de link.

- O acesso remoto à rede da empresa é permitido mediante autenticação segura e controle de acessos.

- A contratação será de forma imediata e totalizada, já contemplando todos os SKUs, suas respectivas quantidades.

- A solução deve fornecer capacidades avançadas de relatórios e monitoramento, permitindo ao TJM-RS acompanhar a eficácia das medidas de segurança utilizadas. Relatórios detalhados sobre incidentes, tentativas de ataque e status de segurança devem ser disponibilizados regularmente;

- A solução deve contribuir para a eficiência operacional do TJM-RS, minimizando o impacto sobre os recursos do sistema e garantindo que o desempenho das estações de trabalho e servidores não seja comprometido.

- A contratação desta solução é imprescindível para assegurar a proteção robusta do ambiente computacional do TJM-RS, atendendo aos mais elevados padrões de segurança cibernética e garantindo a continuidade e eficiência das operações da Justiça Militar. Não serão aceitas licenças provisórias. Somente serão aceitas licenças originais do fabricante dos softwares.

- Indicar pelo menos 1 (um) profissional do seu quadro funcional para fazer ligação com o cliente, durante o horário estabelecido para a prestação do serviço, e responder pela correta execução dos mesmos.

- O suporte técnico deverá ser solicitado em horário comercial através da Central de Atendimento (Help-Desk) da Contratada, conforme os canais oficiais disponibilizados pela empresa contratada, como: 0800 – e-mail, que devem ser fornecidos pela contratada. Entende-se por horário comercial o compreendido entre 08:00hs e 18:00hs, de segundas à sextas- feiras, exceto em feriados.

6. Relatórios e Monitoramento: A solução deve fornecer capacidades avançadas de relatórios e monitoramento, permitindo ao TJM-RS acompanhar a eficácia das medidas de segurança utilizadas. Relatórios detalhados sobre incidentes, tentativas de ataque e status de segurança devem ser disponibilizados regularmente;

7. Eficiência Operacional: A solução deve contribuir para a eficiência operacional do TJM-RS, minimizando o impacto sobre os recursos do sistema e garantindo que o desempenho das estações de trabalho e servidores não seja comprometido.

8. Arquitetura Tecnológica (Configuração):

1. Objeto: Licença da solução de antivírus Kaspersky Next EDR Optimum com gerenciamento.

2. Solução de proteção, detecção e resposta a incidente de endpoint;

2.1. Servidor de Administração e Console Gerenciamento

2.1.1. Compatibilidade:

2.1.1.1. Microsoft Storage Server 2012 e Server R2 x64;

2.1.1.2. Microsoft Windows Server 2012 e R2 Standard / Core / Datacenter x64;

2.1.1.3. Microsoft Windows Server 2016 Standard / Core / Datacenter x64;

2.1.1.4. Microsoft Windows Server 2019 Standard / Core / Datacenter x64;

2.1.1.5. Microsoft Windows Server 2022 Standard / Core / Datacenter x64;

2.1.1.6. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;

2.1.1.7. Microsoft Windows 8 Professional / Enterprise x64;

2.1.1.8. Microsoft Windows 8.1 Professional / Enterprise x32/x64;

2.1.1.9. Microsoft Windows 10 x32/x64;

2.1.1.10. Windows 11 Home / Pro / Enterprise / Education x64;

2.1.2. Suporta as seguintes plataformas virtuais:

1.2.1. Vmware: Workstation 16 Pro, vSphere 6.7, vSphere 7.0;

1.2.2. Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64 e 2022 x64;

1.2.5. Parallels Desktop 17;

1.2.7. Citrix XenServer 7.1, 8.x;

1.2.8. Oracle VM VirtualBox 6;

2.1.3. Características:

2.1.3.1. O console deve ser acessado via WEB (HTTPS) ou MMC;

2.1.3.2. O console deve suportar arquitetura on-premise e arquitetura cloud-based;

2.1.3.3. Console deve ser baseado no modelo cliente/servidor;

2.1.3.4. O console deve suportar autenticação de dois fatores;

2.1.3.5. Deve possuir compatibilidade com Windows Failover Clustering;

2.1.3.6. O servidor de administração deve possui modelo de cluster ativo-passivo;

2.1.3.7. Deve permitir a atribuição de perfis para os administradores da solução de Antivírus;

2.1.3.8. Deve permitir incluir usuários do AD para logarem na console de administração;

2.1.3.9. Console deve ser totalmente integrado com suas funções e módulos, caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, gerenciamento de vulnerabilidades, detecção e resposta de endpoint, avaliação de vulnerabilidades, gerenciamento de dispositivos moveis;

2.1.3.10. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

2.1.3.11. Deverá ser possível buscar novos produtos e soluções a partir da console;

2.1.3.12. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

2.1.3.13. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD.

2.1.3.14. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

2.1.3.15. Deve armazenar histórico das alterações feitas em políticas;

2.1.3.16. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

2.1.3.17. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

2.1.3.18. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

2.1.3.19. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

2.1.3.20 A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

2.1.3.21 Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por sub-rede com os seguintes parâmetros: KB/s e horário;

2.1.3.22. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

2.1.3.23. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

2.1.3.24. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

2.1.3.25. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto;

2.1.3.26. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

2.1.3.27. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

2.1.3.28. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

2.1.3.29. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

2.1.3.30. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

· Nome do computador;

· Nome do domínio;

· Range de IP;

· Sistema Operacional;

· Máquina virtual.

2.1.3.31. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

2.1.3.32. Deve ter a capacidade de descobrir novos dispositivos na rede, utilizando as seguintes técnicas:

2.1.3.32.1. Pesquisa de rede (Windows pooling);

2.1.3.32.2. Pesquisa ativa do AD (AD pooling);

2.1.3.32.3. Pesquisa de IP (IP pooling);

2.1.3.32.4. Pesquisa de rede (Zeroconf pooling);

2.1.3.33. Deve permitir, por meio da console de gerenciamento, extrair um artefato em área de backup de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

2.1.3.34. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

2.1.3.35. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para ser adicionada a proteção;

2.1.3.36. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

2.1.3.37. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

2.1.3.38. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

2.1.3.39. Deve fornecer as seguintes informações dos computadores:

2.1.3.39.1. Se o antivírus está instalado;

2.1.3.39.2. Se o antivírus está iniciado;

2.1.3.39.3. Se o antivírus está atualizado;

2.1.3.39.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

2.1.3.39.5. Minutos/horas desde a última atualização de vacinas;

2.1.3.39.6. Data e horário da última verificação executada na máquina;

2.1.3.39.7. Versão do antivírus instalado na máquina;

2.1.3.39.8. Se for necessário reiniciar o computador para aplicar mudanças;

2.1.3.39.9. Quantidade de vírus encontrados (contador) na máquina;

2.1.3.39.10. Nome do computador;

2.1.3.39.11. Domínio ou grupo de trabalho do computador;

2.1.3.39.12. Data e horário da última atualização de vacinas;

2.1.3.39.13. Sistema operacional com Service Pack;

2.1.3.39.14. Quantidade de processadores;

2.1.3.39.15. Quantidade de memória RAM;

2.1.3.39.16. Sessões de usuários, com informações de contato (caso disponível no Active Directory);

2.1.3.39.17. Endereço IP;

2.1.3.39.18. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

2.1.3.39.19. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD e placa mãe;

2.1.3.39.20. Vulnerabilidades de aplicativos instalados na máquina;

2.1.3.40. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

2.1.3.41. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

2.1.3.41.1. Alteração de Gateway Padrão;

2.1.3.41.2. Alteração de sub-rede;

2.1.3.41.3. Alteração de domínio;

2.1.3.41.4. Alteração de servidor DHCP;

2.1.3.41.5. Alteração de servidor DNS;

2.1.3.41.6. Alteração de servidor WINS;

2.1.3.41.7. Resolução de Nome;

2.1.3.41.8. Disponibilidade de endereço de conexão SSL;

2.1.3.42. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

2.1.3.43. Capacidade de instalar outros servidores administrativos para balancear a carga e aperfeiçoar tráfego de link entre sites diferentes;

2.1.3.44. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

2.1.3.45. O console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores;

2.1.3.46. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

2.1.3.47. Capacidade de herança de configuração de tarefas, políticas e relatórios na estrutura de hierarquia de servidores on-premisse com servidor em cloud.

2.1.3.48. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de aperfeiçoar tráfego da rede;

2.1.3.49. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

2.1.3.50. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

2.1.3.51. Capacidade de monitoramento do sistema através de um SNMP client;

2.1.3.52. Capacidade enviar eventos através de protocolo de syslog;

2.1.3.53. Capacidade exportar eventos para sistemas de SIEM no formato LEEF e CEF.

2.1.3.54. Deve ser capas de enviar os eventos para sistemas de SIEM em canal encriptado.

2.1.3.55. Dever ter a capacidade de exportar eventos para sistemas de SIEM, compatível com Qradar, ArcSight e Splunk.

2.1.3.56. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

2.1.3.57. Listar em um único local, todos os computadores não gerenciados na rede;

2.1.3.58. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e sub-rede;

2.1.3.59. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;

2.1.3.60. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em subnets diferentes do servidor;

2.1.3.61. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

2.1.3.62. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador;

2.1.3.63. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (exe.: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

2.1.3.64. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

2.1.3.65. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

2.1.3.66. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

· Nome do vírus;

· Nome do arquivo infectado;

· Data e hora da detecção;

· Nome da máquina ou endereço IP;

· Ação realizada.

2.1.3.67. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

2.1.3.68. Capacidade de listar updates nas máquinas com o respectivo link para download;

2.1.3.69. Deve criar um backup de todos os arquivos deletados em computadores durante a desinfecção para que possam ser restaurados;

2.1.3.70. Deve ter uma área de backup na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

2.1.3.71. Capacidade de realizar resumo de hardware de cada máquina cliente;

2.1.3.72. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2.2. Sistemas operacionais Windows

2.2.1. Deve ser compatível com os seguintes sistemas de estação de trabalho:

2.2.1.1. Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

2.2.1.2. Microsoft Windows 8 Professional/Enterprise;

2.2.1.3. Microsoft Windows 8.1 Professional / Enterprise;

2.2.1.4. Microsoft Windows 10 Pro / Enterprise / Home / Education;

2.2.1.5. Microsoft Windows 11 Pro / Enterprise / Home / Education;

2.2.2. Deve ser compatível com os seguintes sistemas servidores:

2.2.2.1. Windows Small Business Server 2011 Essentials / Standard (64-bit)

2.2.2.2. Windows MultiPoint Server 2011 (64-bit);

2.2.2.3. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

2.2.2.4. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

2.2.2.5. Windows Server 2016 Essentials / Standard / Datacenter;

2.2.2.6. Windows Server 2019 Essentials / Standard / Datacenter;

2.2.2.7. Windows Server 2022.

2.2.3. Suporta as seguintes plataformas virtuais:

2.2.3.1. Vmware Workstation 16.2.3;

2.2.3.2. Vmware ESXi 7.0 Update 3d;

2.2.3.3. Microsoft Hyper-V Server 2019;

2.2.3.4. Citrix Virtual Apps and Desktops 7 2203;

2.2.3.5. Critrix Provisioning 2203;

2.2.3.6. Citrix Hypervisor 8.2.

2.3. Características:

2.3.1.1. Deve prover as seguintes proteções:

2.3.1.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.3.1.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

2.3.1.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

2.3.1.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

2.3.1.1.5. Deve possui modulo dedicado contra prevenção de intrusão, Prevenção de intrusão do host;

2.3.1.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);

2.3.1.1.7. Controle de dispositivos externos;

2.3.1.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

2.3.1.1.9. Controle de acesso a sites por horário;

2.3.1.1.10. Controle de acesso a sites por usuários;

2.3.1.1.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;

2.3.1.1.12. Controle de execução de aplicativos;

2.3.1.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2.3.1.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.3.1.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

2.3.1.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.3.1.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.3.1.6. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

2.3.1.7. Deverá possuir módulo dedicado para proteção contra port scanning;

2.3.1.8. Deverá possuir módulo dedicado para proteção contra network flooding;

2.3.1.9. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

2.3.1.10. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

2.3.1.11. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

2.3.1.12. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

2.3.1.13. Deverá possuir módulo para proteção contra malwares que tenta realizar criptografia de arquivos em pastas compartilhadas.

2.3.1.14. Deve ter a capacidade de detectar ameaças instaladas na BIOS ROM do endpoint.

2.3.1.15. Deverá realizar scanner de firmaware em busca de rootkits.

2.3.1.16. Ao detectar uma ameaça, a solução deve exibir informações:

2.3.1.17. Do objeto SHA256;

2.3.1.18. Do objeto MD5.

2.3.1.19. Capacidade de verificar somente arquivos novos e alterados;

2.3.1.20. Capacidade de verificar objetos usando heurística;

2.3.1.21. Capacidade de agendar uma pausa na verificação;

2.3.1.22. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

2.3.1.23. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

2.3.1.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.3.1.24.1. Perguntar o que fazer, ou;

2.3.1.24.2. Bloquear acesso ao objeto;

2.3.1.24.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.1.24.2.2. Caso positivo de desinfecção:

2.3.1.24.2.2.1. Restaurar o objeto para uso;

2.3.1.24.2.3. Caso negativo de desinfecção:

2.3.1.24.2.3.1. Mover para uma área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.1.25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

2.3.1.26. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

2.3.1.27. Capacidade de verificar links inseridos em e-mails contra phishings;

2.3.1.28. Capacidade de verificar todo o tráfego web de acessos à internet nos protocolos HTTP, HTTPS e FTP, utilizando técnicas de banco de dados, serviços da nuvem do fabricante e analise de heurística bloqueada arquivos, sites de phishing e URL maliciosas;

2.3.1.29. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

2.3.1.30. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

2.3.1.30.1. Perguntar o que fazer, ou;

2.3.1.30.2. Bloquear o e-mail;

2.3.1.30.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.1.30.2.2. Caso positivo de desinfecção:

2.3.1.30.2.3. Restaurar o e-mail para o usuário;

2.3.1.30.2.4. Caso negativo de desinfecção:

2.3.1.30.2.4.1. Mover para uma área de backup ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.1.31. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

2.3.1.32. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

2.3.1.33. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc);

2.3.1.34. Deve ser possível realizar o monitoramento das atividades de rede em tempo real, visualizando portas UDP/TCP e Trafego de rede por aplicativo.

2.3.1.35. Capacidade de alterar as portas monitoradas pelos módulos de ameaças web, controle de acesso à web e e-mail;

2.3.1.36. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

2.3.1.36.1. Perguntar o que fazer, ou;

2.3.1.36.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.3.1.36.3. Permitir acesso ao objeto;

2.3.1.37. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

2.3.1.37.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

2.3.1.37.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

2.3.1.38. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

2.3.1.39. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

2.3.1.40. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

2.3.1.41. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);

2.3.1.42. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

2.3.1.43. Deve possuir módulo para proteção contra port scans, network flooding e MAC spoofing. A base de dados de análise deve ser atualizada juntamente com as vacinas;

2.3.1.44. Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;

2.3.1.45. Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.

2.3.1.46. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.3.1.46.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.3.1.46.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.3.1.47 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

2.3.1.47.1. Discos de armazenamento locais;

2.3.1.47.2. Armazenamento removível;

2.3.1.47.3. Impressoras;

2.3.1.47.4. CD/DVD;

2.3.1.47.5. Modems;

2.3.1.47.6. Dispositivos multifuncionais;

2.3.1.47.7. Leitores de smart card;

2.3.1.47.8. Wi-Fi;

2.3.1.47.9. Adaptadores de rede externos;

2.3.1.47.10. Dispositivos MP3 ou smartphones;

2.3.1.47.11. Dispositivos Bluetooth;

2.3.1.47.12. Câmeras e Scanners.

2.3.1.48. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

2.3.1.49. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

2.3.1.50. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

2.3.1.51. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras.

2.3.1.52. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.

2.3.1.53. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

2.3.1.54. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

2.3.1.55. Ter a capacidade de detectar a modificação de firmware em dispositivos USB mal-intencionado.

2.3.1.56. Deverá realizar a validação dos dispositivos que se conectam via USB que emulam teclados;

2.3.1.57. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

2.3.1.57.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.3.1.57.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.3.1.58. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

2.3.1.59. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

2.3.1.60. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

2.3.1.61. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.3.1.62. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

2.3.1.63. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

2.3.1.64. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.3.1.65. Capacidade de integração com a Antimalware Scan Interface (AMSI).

2.3.1.66. Deve permitir realizar o gerenciamento por meio de integração via REST API.

2.3.1.67. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.

2.4. Estações Mac OS X

2.4.1. Compatibilidade:

2.4.1.1. macOS Mojave 10.14

2.4.1.2. macOS Catalina 10.15

2.4.1.3. macOS Big Sur 11.0

2.4.1.4. macOS Monterey 12

2.4.2. Características:

2.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;

2.4.2.3. Possuir módulo de bloqueio á ataques na rede;

2.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

2.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;

2.4.2.6. Possibilidade de importar uma chave no pacote de instalação;

2.4.2.7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.4.2.8. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

2.4.2.9. Capacidade de voltar para a base de dados de vacina anterior;

2.4.2.10. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.4.2.11. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

2.4.2.12. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

2.4.2.13. Capacidade de verificar somente arquivos novos e alterados;

2.4.2.14. Capacidade de verificar objetos usando heurística;

2.4.2.15. Capacidade de agendar uma pausa na verificação;

2.4.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.4.2.16.1. Perguntar o que fazer, ou;

2.4.2.16.2. Bloquear acesso ao objeto;

2.4.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.4.2.16.2.2. Caso positivo de desinfecção:

2.4.2.16.2.1. Restaurar o objeto para uso;

2.4.2.16.2.2. Caso negativo de desinfecção:

2.4.2.16.2.3. Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.4.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

2.4.2.18. Capacidade de verificar arquivos de formato de email;

2.4.2.18. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

2.4.2.19.Capacidade de, através da mesma console central de gerenciamento:

2.4.2.19.1. Ser instalado;

2.4.2.19.2. Ser removido;

2.4.2.19.3. Ser gerenciado;

2.5. Sistemas operacionais Linux

2.5.1. Compatibilidade:

2.5.1.1. Plataforma 32-bits:

2.5.1.1.1. Red Hat Linux 6.7 e superior;

2.5.1.1.2. CentOS 6.7 e superior;

2.5.1.1.3. Debian 9.4 e superior;

2.5.1.1.4. Debian 10.1 e superior;

2.5.1.1.5. Debian 11.1 e superior;

2.5.1.1.6. Linux Mint 19 e superior;

2.5.1.1.7. Mageia 4;

2.5.1.2. Plataforma 64-bits:

2.5.1.2.1. Ubuntu 18.04 e superior;

2.5.1.2.2. Ubuntu 20.04;

2.5.1.2.3. Red Hat Enterprise Linux 6.7;

2.5.1.2.4. Red Hat Enterprise Linux 7.2;

2.5.1.2.5. Red Hat Enterprise Linux 8.0;

2.5.1.2.6. CentOS 6.7 e superior;

2.5.1.2.7. CentOS 7.2 e superior;

2.5.1.2.8. CentOS 8.0 e superior;

2.5.1.2.9. Debian 9.4 e superior;

2.5.1.2.10. Debian 10.1 e superior;

2.5.1.2.11. OracleLinux 7.3 e superior;

2.5.1.2.12. OracleLinux 8 e sueperior;

2.5.1.2.13. SUSE Server 12 e superior;

2.5.1.2.14. SUSE Server 15 e superior;

2.5.1.2.15. openSUSE Leap 15;

2.5.1.2.16. Amazon Linux 2;

2.5.1.2.17. Linux Mint 19 e superior;

2.5.1.2.18. Linux Mint 20.1 e superior;

2.5.1.2.19. Oracle Linux 7.3 e superior;

2.5.1.2.20. Oracle Linux 8.0 e superior;

2.5.1.2.21. RED OS 7.2;

2.6. Características:

2.6.1.1. Deve prover as seguintes proteções:

2.6.1.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.6.1.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:

2.6.1.3.1. Via linha de comando;

2.6.1.3.2. Via console administrativa;

2.6.1.3.3. Via GUI;

2.6.1.3.4. Via web (remotamente);

2.6.1.4. Deve possuir funcionalidade de scan de drives removíveis, tais como:

2.6.1.4.1. CDs;

2.6.1.4.2. DVDs;

2.6.1.4.3. Discos blu-ray;

2.6.1.4.4. Flash drives (pen drives);

2.6.1.4.5. HDs externos;

2.6.1.4.6. Disquetes;

2.6.1.5. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:

2.6.1.5.1. Por tipo de dispositivo;

2.6.1.5.2. Por barramento de conexão.

2.6.1.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

2.6.1.7. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.6.1.7.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

2.6.1.7.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

2.6.1.7.3. Leitura de configurações;

2.6.1.7.4. Modificação de configurações;

2.6.1.7.5. Gerenciamento de Backup;

2.6.1.7.6. Visualização de logs;

2.6.1.7.7. Gerenciamento de logs;

2.6.1.7.8. Gerenciamento de ativação da aplicação;

2.6.1.7.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

2.6.1.8. Capacidade de criar exclusões por local, máscara e nome da ameaça;

2.6.1.9. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

2.6.1.10. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

2.6.1.11. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

2.6.1.12. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

2.6.1.12.1. Alta;

2.6.1.12.2. Média;

2.6.1.12.3. Baixa;

2.6.1.12.4. Recomendado;

2.6.1.13. Gerenciamento de backup de arquivos: Fazer backup de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de backup;

2.6.1.14. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

2.6.1.15. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

2.6.1.16. Capacidade de definir o consumo de recursos nas varreduras para não impactar outros aplicativos que necessitem de mais

recursos de memória ou processamento;

2.6.1.17. Deverá ser possível priorizar a execução de tarefas;

2.6.1.18. Capacidade de verificar objetos usando heurística;

2.6.1.19. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em malicioso;

2.6.1.20. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP;

2.6.1.21. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

2.6.1.21.1. Detecção de phishing e sites maliciosos;

2.6.1.21.2. Bloqueio de download de arquivos maliciosos;

2.6.1.22.3. Bloqueio de adware;

2.6.1.22.4. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

2.6.1.22. Deve fornecer a possibilidade de administração remota através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux);

2.6.1.23. Deverá fornecer informações de todas as executáveis das aplicações;

2.6.1.24. Deve possuir módulo de proteção contra criptografia maliciosa.

2.6.1.25. Deverá possuir controle de execução de aplicações;

2.6.1.26. O modulo de controle de aplicação deverá possuir as seguintes funcionalidades:

2.6.1.26.1. Criação de lista de bloqueio de aplicação;

2.6.1.26.2. Criação de lista de permissão de aplicação;

2.6.1.27. Deverá realizar busca de ameaças em setores críticos do sistema operacional:

2.6.1.27.1. Setor de inicialização;

2.6.1.27.2. Objetos de inicialização;

2.6.1.27.3. Processos de memória;

2.6.1.27.4. Memória do kernel;

2.7. Compatibilidade com servidores windows;

2.7.1. Compatibilidade de sistema legado:

2.7.2. Plataforma x32 ou x64:

2.7.2.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;

2.7.2.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;

2.7.3. Características:

2.7.3.1. Deve prover as seguintes proteções:

2.7.3.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.7.3.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;

2.7.3.1.3. Firewall com IDS;

2.7.3.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2.7.3.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.7.3.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:

2.7.3.3.1. Via console administrativo;

2.7.3.3.2. Via web (remotamente);

2.7.3.4. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

2.7.3.5. Deverá ter a capacidade de customizar o uso de CPU para realização de scanner no dispositivo.

2.7.3.6. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.7.3.6.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

2.7.3.6.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

2.7.3.6.3. Leitura de configurações;

2.7.3.6.4. Modificação de configurações;

2.7.3.6.5. Gerenciamento de backup;

2.7.3.6.6. Visualização de logs;

2.7.3.6.7. Gerenciamento de logs;

2.7.3.6.8. Gerenciamento de ativação da aplicação;

2.7.3.6.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

2.7.3.6.10. Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.

2.7.3.7. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.7.3.7.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.7.3.7.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.7.3.8. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

2.7.3.9. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;

2.7.3.10. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);

2.7.3.11. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

2.7.3.12. Deve possuir funcionalidade de análise personalizada de logs do Windows.

2.7.3.13. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

2.7.3.14. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

2.7.3.15. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

2.7.3.16. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.7.3.17. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.7.3.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

2.7.3.19. Capacidade de verificar somente arquivos novos e alterados;

2.7.3.20. Capacidade de escolher qual tipo de objeto composto será verificada (ex: arquivos comprimidos, arquivos auto descompressores, PST, arquivos compactados por compactadores binários, etc.);

2.7.3.21. Capacidade de verificar objetos usando heurística;

2.7.3.22. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

2.7.3.23. Capacidade de agendar uma pausa na verificação;

2.7.3.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.7.3.24.1. Perguntar o que fazer, ou;

2.7.3.24.2. Bloquear acesso ao objeto;

2.7.3.24.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.7.3.24.2.2. Caso positivo de desinfecção:

2.7.3.24.2.2.1. Restaurar o objeto para uso;

2.7.3.24.2.3. Caso negativo de desinfecção:

2.7.3.24.2.3.1. Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.7.3.25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

2.7.3.26. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos maliciosos em área de backup;

2.7.3.27. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

2.7.3.28. Em caso de detecção de sinais de uma infecção ativa, deve possuir capacidade de, automaticamente:

2.7.3.28.1. Executar os procedimentos pré-configurados pelo administrador;

2.7.3.28.2. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.

2.7.3.29. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

2.7.3.30. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

2.7.3.31. Capacidade de detectar anomalias no comportamento de um software usando análise heurística.

2.7.3.32. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

2.7.3.33. Deve possuir controle de dispositivos externos.

2.8. Smartphones e tablets

2.8.1. Compatibilidade:

2.8.1. Suportar o Android das versões: 5.0 ao 12.

2.8.2. Características:

2.8.2.1. Deve prover as seguintes proteções:

2.8.2.1.1 Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

2.8.2.1.2. Proteção contra adware e autodialers;

2.8.2.1.3. Todos os objetos transmitidos;

2.8.2.1.4. Arquivos abertos no smartphone;

2.8.2.1.5. Programas instalados usando a interface do smartphone

2.8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

2.8.2.2 Deverão isolar em área de backup os arquivos infectados;

2.8.2.3. Deverá atualizar as bases de vacinas de modo agendado;

2.8.2.4. Capacidade de desativar por política:

2.8.2.4.1. Wi-fi;

2.8.2.4.2. Câmera;

2.8.2.4.3. Bluetooth.

2.8.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

2.8.2.6 Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

2.8.2.6. Deverá ter firewall pessoal;

2.8.2.6. Capacidade de tirar fotos quando a senha for inserida incorretamente;

2.8.2.7. Capacidade de enviar comandos remotamente de:

2.8.2.7.1. Localizar;

2.8.2.7.2. Bloquear.

2.8.2.7.3. Capacidade de detectar Root nos dispositivos;

2.8.2.7.4. Capacidade de bloquear o acesso a site por categoria em dispositivos;

2.8.2.7.5. Capacidade de bloquear o acesso a sites phishing ou maliciosos;

2.8.2.7.6. Capacidade de configurar White e blacklist de aplicativos;

2.8.2.7.7. Capacidade de localizar o dispositivo quando necessário;

2.8.2.7.8. Permitir atualização das definições quando estiver em “roaming”;

2.8.2.7.9. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

2.8.2.7.9. Capacidade de agendar uma verificação;

2.8.2.7.10. Capacidade de enviar URL de instalação por e-mail;

2.8.2.7.11. Capacidade de fazer a instalação do agente através de um link QRCode;

2.8.2.7.12. Capacidade de executar as seguintes ações caso a desinfecção falhe:

ü Deletar;

ü Ignorar;

ü Fazer backup;

ü Perguntar ao usuário.

2.8.3. Gerenciamento de dispositivos móveis (MDM) – Android:

2.8.3.1. Compatibilidade:

2.8.3.1.1. Dispositivos com os sistemas operacionais:

2.8.3.1.1.1. Do Android versão 5.0 a 12

2.8.3.1.1.2. Deverá possuir integração com sistemas de gerenciamentos:

2.8.3.1.2.1. VMWare AirWatch 9.3;

2.8.3.1.2.2. MobileIron;

2.8.3.1.2.3. IBM Maas360;

2.8.3.1.2.4. Microsoft Intune;

2.8.3.1.2.5. SOTI MobiControl;

2.8.3.2 Características:

2.8.3.2.1. Capacidade de aplicar políticas de Activesync através do servidor Microsoft Exchange;

2.8.3.2.2. Capacidade de ajustar as configurações de:

2.8.3.2.2.1. Sincronização de e-mail;

2.8.3.2.2.2. Uso de aplicativos;

2.8.3.2.2.3. Senha do usuário;

2.8.3.2.2.4. Criptografia de dados;

2.8.3.2.2.5. Conexão de mídia removível.

2.8.3.2.2.6. Capacidade de instalar certificados digitais em dispositivos móveis;

2.8.3.2.2.7. Deve permitir configurar horário para sincronização do dispositivo com o console de gerenciamento;

2.8.3.2.2.8. Capacidade de desinstalar remotamente o antivírus do dispositivo;

2.8.3.2.2.9. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;

2.8.3.2.2.10 Capacidade de sincronizar com Samsung Knox;

2.8.4. Gerenciamento de dispositivos móveis (MDM) – iOS

2.8.4.1. Compatibilidade:

2.8.4.1.1. Ser compatível com dispositivos com os sistemas operacionais:

2.8.4.1.1.1. iOS 10.0 – 10.3.3

2.8.4.1.1.2. iOS 11.0 – 11.3

2.8.4.1.1.3. iOS 12.0

2.8.4.1.1.4. iOS 13.0

2.8.4.1.1.5. IPadOS 13 ao 15

2.8.4.1.2 Características:

2.8.4.1.2.1. Capacidade de aplicar políticas de Activesync através do servidor Microsoft Exchange;

2.8.4.1.3. Capacidade de ajustar as configurações de:

2.8.4.1.3.1. Sincronização de e-mail;

2.8.4.1.3.2 Senha do usuário;

2.8.4.1.3.3 Criptografia de dados;

2.8.4.1.3.4 Capacidade de instalar certificados digitais em dispositivos móveis;

2.8.4.1.3.5 Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos clientes através de:

2.8.4.1.3.5.1. Link por e-mail;

2.8.4.1.3.5 .2 Link por mensagem de texto;

2.8.4.1.3.5.3 QR Code

2.8.4.1.3.6 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

2.8.4.1.3.7 Capacidade de, remotamente, bloquear um dispositivo iOS;

2.9 Criptografia

2.9.1. Compatibilidade:

2.9.1.2. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;

2.9.1.3. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;

2.9.1.4. Microsoft Windows 7 Professional SP1 ou superior x86/x64;

2.9.1.5. Microsoft Windows 8 Enterprise x86/x64;

2.9.1.6. Microsoft Windows 8 Pro x86/x64;

2.9.1.7. Microsoft Windows 8.1 Pro x86/x64;

2.9.1.8. Microsoft Windows 8.1 Enterprise x86/x64;

2.9.1.9. Microsoft Windows 10 Enterprise x86/x64;

2.9.1.10. Microsoft Windows 10 Pro x86/x64;

2.9.2. Características:

2.9.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

2.9.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

2.9.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

2.9.2.4. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;

2.9.2.5. Permitir criar vários usuários de autenticação pré-boot;

2.9.2.6. Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real;

2.9.2.7. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

2.9.2.8. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

2.9.2.9. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

2.9.2.10. Criptografar todos os arquivos individualmente;

2.9.2.11. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

2.9.2.12. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

2.9.2.13. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente;

2.9.2.14. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

2.9.3. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

2.9.4. Verifica compatibilidade de hardware antes de aplicar a criptografia;

2.9.5. Possibilita estabelecer parâmetros para a senha de criptografia;

2.9.6. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

2.9.7. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo;

2.9.8. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

2.9.9 Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

2.9.10. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;

2.9.11. Permite criar um grupo de extensões de arquivos a serem criptografados;

2.9.12. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

2.9.13. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

2.9.14. Capacidade de deletar arquivos de forma segura após a criptografia;

2.9.15. Capacidade de criptografar somente o espaço em disco utilizado;

2.9.16. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

2.9.17. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

2.9.18. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;

2.9.19. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

2.9.20. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

2.9.21. Capacidade de fazer “Hardware encryption”;

2.10. Gerenciamento de Sistemas

2.10.1.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;

2.10.1.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

2.10.1.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

2.10.1.4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

2.10.1.5. Capacidade de gerenciar licenças de softwares de terceiros;

2.10.1.6. Capacidade de atualizar informações sobre hardware presentes nos relatórios após mudanças de hardware nas máquinas gerenciadas;

2.10.1.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc);

2.10.2 Possibilita fazer distribuição de software de forma manual e agendada;

2.10.3 Suporta modo de instalação silenciosa;

2.10.4 Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

2.10.1.5 Possibilita fazer a distribuição através de agentes de atualização;

2.10.1.6 Utiliza tecnologia multicast para evitar tráfego na rede;

2.10.1.7 Possibilita criar um inventário centralizado de imagens;

2.10.1.8. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

2.10.1.9. Suporte a WakeOnLan para deploy de imagens;

2.10.1.10. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

2.10.1.11. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

2.10.1.12 Capacidade de gerar relatórios de vulnerabilidades e patches;

2.10.1.13 Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

2.10.1.14 Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

2.10.1.15 Permite baixar atualizações para o computador sem efetuar a instalação;

2.10.1.16 Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

2.10.1.17 Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

2.10.1.18 Permite selecionar produtos a serem atualizados pela console de gerenciamento;

2.10.1.18 Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança,

ferramentas, drivers, etc;

2.10.1.19 Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

2.10.1.20 Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

2.10.1.21 Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;

2.10.1.22 Deve permitir selecionar o idioma das aplicações que serão atualizadas;

2.10.1.23 Permitir agendar o sincronismo entre o console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

2.11 Detecção e Resposta

2.11.1. Compatibilidade:

2.11.1.1 Deve ser compatível com os seguintes sistemas de estação de trabalho:

2.11.1.1.1 Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

2.11.1.1.2 Microsoft Windows 8 Professional/Enterprise;

2.11.1.1.3 Microsoft Windows 8.1 Professional / Enterprise;

2.11.1.1.4 Microsoft Windows 10 Pro / Enterprise / Home / Education;

2.11.1.1.5 Microsoft Windows 11 Pro / Enterprise / Home / Education;

2.11.1.1.6 Deve ser compatível com os seguintes sistemas servidores:

2.11.1.1.6.1 Windows Small Business Server 2011 Essentials / Standard (64-bit)

2.11.1.1.6.2. Windows MultiPoint Server 2011 (64-bit);

2.11.1.1.6.3. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

2.11.1.1.6.4. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

2.11.1.1.6.5. Windows Server 2016 Essentials / Standard / Datacenter;

2.11.1.1.6.6. Windows Server 2019 Essentials / Standard / Datacenter;

2.11.1.1.6.7. Windows Server 2022.

2.11.2. Características

2.11.2.1 As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;

2.11.2.2 A solução deve oferecer módulo focado em capacidades de EDR “Endpoint Detection and Response”, incluindo no mínimo as seguintes capacidades:

2.11.2.3 O agente deve ter capacidade de coletar e processar dados relacionados ao veredito e ao contexto da ameaça;

2.11.2.4 Deve fornecer graficamente a visualização da cadeia do ataque;

2.11.2.5 Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).

2.11.3. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

2.11.3.1. Isolar o host;

2.11.3.2. Iniciar uma varredura nas áreas críticas;

2.11.3.3. Quarentenar o objeto;

2.11.4 A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

2.11.5 Visibilidade das detecções provenientes de endpoint;

2.11.5.1. Processos;

2.11.5.2. Conexões remotas;

2.11.5.3 Alterações de registros;

2.11.5.4 Objetos baixados

2.11.6 Capacidade de integração com a solução de sandbox cloud do fabricante;

2.11.7 Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.

2.11.8 Deverá possuir informações de assinaturas digitais da ameaça;

2.11.9 Deve ser capaz de trazer informações do arquivo sobre sua geolocalização;

2.11.10 Possibilidade de informar quando o arquivo foi detectado pela base de conhecimento;

2.11.11 Trazer a identificação de comportamento e/ou descrição sobre o arquivo;

2.11.12 A solução deve oferecer no mínimo as seguintes opções de resposta:

2.11.12.1 Prevenir a execução de um arquivo;

2.11.12.2. Quarentenar um arquivo;

2.11.12.3. Iniciar uma varredura por IoC;

2.11.12.4. Parar um processo;

2.11.12.5. Executar um processo;

2.11.13 Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

2.11.13.1 A opção de isolamento deve estar disponível junto a visualização do incidente;

2.11.13.2 Na analise do incidente a ferramenta deverá apresentar recomendações de ações que o analista precisa executar para remediar o incidente;

2.11.13.3 As recomendações devem ser guiadas juntamente com guias das opções selecionadas pelo analista, apresentando pop-up guiando as ações.

2.11.13.4 Deverá ser possível remover a máquina do isolamento a partir do incidente;

2.11.13.5 Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

2.11.13.6 Deve oferecer informações de inteligência de ameaças do próprio fabricante;

2.11.13.7 Deverá possuir detecção baseada em sandbox do tipo cloud;

2.11.13. 8 Deverá suportar IoC de terceiros em formatos OpenIOC.

2.1.1. Compatibilidade:

2.1.1.1. Microsoft Storage Server 2012 e Server R2 x64;

2.1.1.2. Microsoft Windows Server 2012 e R2 Standard / Core / Datacenter x64;

2.1.1.3. Microsoft Windows Server 2016 Standard / Core / Datacenter x64;

2.1.1.4. Microsoft Windows Server 2019 Standard / Core / Datacenter x64;

2.1.1.5. Microsoft Windows Server 2022 Standard / Core / Datacenter x64;

2.1.1.6. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;

2.1.1.7. Microsoft Windows 8 Professional / Enterprise x64;

2.1.1.8. Microsoft Windows 8.1 Professional / Enterprise x32/x64;

2.1.1.9. Microsoft Windows 10 x32/x64;

2.1.1.10. Windows 11 Home / Pro / Enterprise / Education x64;

2.1.2. Suporta as seguintes plataformas virtuais:

1.2.1. Vmware: Workstation 16 Pro, vSphere 6.7, vSphere 7.0;

1.2.2. Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64 e 2022 x64;

1.2.5. Parallels Desktop 17;

1.2.7. Citrix XenServer 7.1, 8.x;

1.2.8. Oracle VM VirtualBox 6;

2.1.3. Características:

2.1.3.1. O console deve ser acessado via WEB (HTTPS) ou MMC;

2.1.3.2. O console deve suportar arquitetura on-premise e arquitetura cloud-based;

2.1.3.3. Console deve ser baseado no modelo cliente/servidor;

2.1.3.4. O console deve suportar autenticação de dois fatores;

2.1.3.5. Deve possuir compatibilidade com Windows Failover Clustering;

2.1.3.6. O servidor de administração deve possui modelo de cluster ativo-passivo;

2.1.3.7. Deve permitir a atribuição de perfis para os administradores da solução de Antivírus;

2.1.3.8. Deve permitir incluir usuários do AD para logarem na console de administração;

2.1.3.9. Console deve ser totalmente integrado com suas funções e módulos, caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, gerenciamento de vulnerabilidades, detecção e resposta de endpoint, avaliação de vulnerabilidades, gerenciamento de dispositivos moveis;

2.1.3.10. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

2.1.3.11. Deverá ser possível buscar novos produtos e soluções a partir da console;

2.1.3.12. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

2.1.3.13. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD.

2.1.3.14. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

2.1.3.15. Deve armazenar histórico das alterações feitas em políticas;

2.1.3.16. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

2.1.3.17. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

2.1.3.18. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

2.1.3.19. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

2.1.3.20 A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

2.1.3.21 Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por sub-rede com os seguintes parâmetros: KB/s e horário;

2.1.3.22. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

2.1.3.23. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

2.1.3.24. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

2.1.3.25. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto;

2.1.3.26. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

2.1.3.27. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

2.1.3.28. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

2.1.3.29. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

2.1.3.30. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

· Nome do computador;

· Nome do domínio;

· Range de IP;

· Sistema Operacional;

· Máquina virtual.

2.1.3.31. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

2.1.3.32. Deve ter a capacidade de descobrir novos dispositivos na rede, utilizando as seguintes técnicas:

2.1.3.32.1. Pesquisa de rede (Windows pooling);

2.1.3.32.2. Pesquisa ativa do AD (AD pooling);

2.1.3.32.3. Pesquisa de IP (IP pooling);

2.1.3.32.4. Pesquisa de rede (Zeroconf pooling);

2.1.3.33. Deve permitir, por meio da console de gerenciamento, extrair um artefato em área de backup de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

2.1.3.34. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

2.1.3.35. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para ser adicionada a proteção;

2.1.3.36. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

2.1.3.37. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

2.1.3.38. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

2.1.3.39. Deve fornecer as seguintes informações dos computadores:

2.1.3.39.1. Se o antivírus está instalado;

2.1.3.39.2. Se o antivírus está iniciado;

2.1.3.39.3. Se o antivírus está atualizado;

2.1.3.39.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

2.1.3.39.5. Minutos/horas desde a última atualização de vacinas;

2.1.3.39.6. Data e horário da última verificação executada na máquina;

2.1.3.39.7. Versão do antivírus instalado na máquina;

2.1.3.39.8. Se for necessário reiniciar o computador para aplicar mudanças;

2.1.3.39.9. Quantidade de vírus encontrados (contador) na máquina;

2.1.3.39.10. Nome do computador;

2.1.3.39.11. Domínio ou grupo de trabalho do computador;

2.1.3.39.12. Data e horário da última atualização de vacinas;

2.1.3.39.13. Sistema operacional com Service Pack;

2.1.3.39.14. Quantidade de processadores;

2.1.3.39.15. Quantidade de memória RAM;

2.1.3.39.16. Sessões de usuários, com informações de contato (caso disponível no Active Directory);

2.1.3.39.17. Endereço IP;

2.1.3.39.18. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

2.1.3.39.19. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD e placa mãe;

2.1.3.39.20. Vulnerabilidades de aplicativos instalados na máquina;

2.1.3.40. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

2.1.3.41. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

2.1.3.41.1. Alteração de Gateway Padrão;

2.1.3.41.2. Alteração de sub-rede;

2.1.3.41.3. Alteração de domínio;

2.1.3.41.4. Alteração de servidor DHCP;

2.1.3.41.5. Alteração de servidor DNS;

2.1.3.41.6. Alteração de servidor WINS;

2.1.3.41.7. Resolução de Nome;

2.1.3.41.8. Disponibilidade de endereço de conexão SSL;

2.1.3.42. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

2.1.3.43. Capacidade de instalar outros servidores administrativos para balancear a carga e aperfeiçoar tráfego de link entre sites diferentes;

2.1.3.44. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

2.1.3.45. O console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores;

2.1.3.46. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

2.1.3.47. Capacidade de herança de configuração de tarefas, políticas e relatórios na estrutura de hierarquia de servidores on-premisse com servidor em cloud.

2.1.3.48. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de aperfeiçoar tráfego da rede;

2.1.3.49. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

2.1.3.50. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

2.1.3.51. Capacidade de monitoramento do sistema através de um SNMP client;

2.1.3.52. Capacidade enviar eventos através de protocolo de syslog;

2.1.3.53. Capacidade exportar eventos para sistemas de SIEM no formato LEEF e CEF.

2.1.3.54. Deve ser capas de enviar os eventos para sistemas de SIEM em canal encriptado.

2.1.3.55. Dever ter a capacidade de exportar eventos para sistemas de SIEM, compatível com Qradar, ArcSight e Splunk.

2.1.3.56. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

2.1.3.57. Listar em um único local, todos os computadores não gerenciados na rede;

2.1.3.58. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e sub-rede;

2.1.3.59. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;

2.1.3.60. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em subnets diferentes do servidor;

2.1.3.61. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

2.1.3.62. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador;

2.1.3.63. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (exe.: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

2.1.3.64. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

2.1.3.65. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

2.1.3.66. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

· Nome do vírus;

· Nome do arquivo infectado;

· Data e hora da detecção;

· Nome da máquina ou endereço IP;

· Ação realizada.

2.1.3.67. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

2.1.3.68. Capacidade de listar updates nas máquinas com o respectivo link para download;

2.1.3.69. Deve criar um backup de todos os arquivos deletados em computadores durante a desinfecção para que possam ser restaurados;

2.1.3.70. Deve ter uma área de backup na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

2.1.3.71. Capacidade de realizar resumo de hardware de cada máquina cliente;

2.1.3.72. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2.2. Sistemas operacionais Windows

2.2.1. Deve ser compatível com os seguintes sistemas de estação de trabalho:

2.2.1.1. Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

2.2.1.2. Microsoft Windows 8 Professional/Enterprise;

2.2.1.3. Microsoft Windows 8.1 Professional / Enterprise;

2.2.1.4. Microsoft Windows 10 Pro / Enterprise / Home / Education;

2.2.1.5. Microsoft Windows 11 Pro / Enterprise / Home / Education;

2.2.2. Deve ser compatível com os seguintes sistemas servidores:

2.2.2.1. Windows Small Business Server 2011 Essentials / Standard (64-bit)

2.2.2.2. Windows MultiPoint Server 2011 (64-bit);

2.2.2.3. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

2.2.2.4. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

2.2.2.5. Windows Server 2016 Essentials / Standard / Datacenter;

2.2.2.6. Windows Server 2019 Essentials / Standard / Datacenter;

2.2.2.7. Windows Server 2022.

2.2.3. Suporta as seguintes plataformas virtuais:

2.2.3.1. Vmware Workstation 16.2.3;

2.2.3.2. Vmware ESXi 7.0 Update 3d;

2.2.3.3. Microsoft Hyper-V Server 2019;

2.2.3.4. Citrix Virtual Apps and Desktops 7 2203;

2.2.3.5. Critrix Provisioning 2203;

2.2.3.6. Citrix Hypervisor 8.2.

2.3. Características:

2.3.1.1. Deve prover as seguintes proteções:

2.3.1.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.3.1.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

2.3.1.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

2.3.1.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

2.3.1.1.5. Deve possui modulo dedicado contra prevenção de intrusão, Prevenção de intrusão do host;

2.3.1.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);

2.3.1.1.7. Controle de dispositivos externos;

2.3.1.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

2.3.1.1.9. Controle de acesso a sites por horário;

2.3.1.1.10. Controle de acesso a sites por usuários;

2.3.1.1.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;

2.3.1.1.12. Controle de execução de aplicativos;

2.3.1.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2.3.1.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.3.1.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

2.3.1.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.3.1.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de

adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.3.1.6. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

2.3.1.7. Deverá possuir módulo dedicado para proteção contra port scanning;

2.3.1.8. Deverá possuir módulo dedicado para proteção contra network flooding;

2.3.1.9. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

2.3.1.10. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

2.3.1.11. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

2.3.1.12. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

2.3.1.13. Deverá possuir módulo para proteção contra malwares que tenta realizar criptografia de arquivos em pastas compartilhadas.

2.3.1.14. Deve ter a capacidade de detectar ameaças instaladas na BIOS ROM do endpoint.

2.3.1.15. Deverá realizar scanner de firmaware em busca de rootkits.

2.3.1.16. Ao detectar uma ameaça, a solução deve exibir informações:

2.3.1.17. Do objeto SHA256;

2.3.1.18. Do objeto MD5.

2.3.1.19. Capacidade de verificar somente arquivos novos e alterados;

2.3.1.20. Capacidade de verificar objetos usando heurística;

2.3.1.21. Capacidade de agendar uma pausa na verificação;

2.3.1.22. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

2.3.1.23. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

2.3.1.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.3.1.24.1. Perguntar o que fazer, ou;

2.3.1.24.2. Bloquear acesso ao objeto;

2.3.1.24.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.1.24.2.2. Caso positivo de desinfecção:

2.3.1.24.2.2.1. Restaurar o objeto para uso;

2.3.1.24.2.3. Caso negativo de desinfecção:

2.3.1.24.2.3.1. Mover para uma área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.1.25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

2.3.1.26. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

2.3.1.27. Capacidade de verificar links inseridos em e-mails contra phishings;

2.3.1.28. Capacidade de verificar todo o tráfego web de acessos à internet nos protocolos HTTP, HTTPS e FTP, utilizando técnicas de banco de dados, serviços da nuvem do fabricante e analise de heurística bloqueada arquivos, sites de phishing e URL maliciosas;

2.3.1.29. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

2.3.1.30. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

2.3.1.30.1. Perguntar o que fazer, ou;

2.3.1.30.2. Bloquear o e-mail;

2.3.1.30.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.1.30.2.2. Caso positivo de desinfecção:

2.3.1.30.2.3. Restaurar o e-mail para o usuário;

2.3.1.30.2.4. Caso negativo de desinfecção:

2.3.1.30.2.4.1. Mover para uma área de backup ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.1.31. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

2.3.1.32. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

2.3.1.33. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc);

2.3.1.34. Deve ser possível realizar o monitoramento das atividades de rede em tempo real, visualizando portas UDP/TCP e Trafego de rede por aplicativo.

2.3.1.35. Capacidade de alterar as portas monitoradas pelos módulos de ameaças web, controle de acesso à web e e-mail;

2.3.1.36. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

2.3.1.36.1. Perguntar o que fazer, ou;

2.3.1.36.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.3.1.36.3. Permitir acesso ao objeto;

2.3.1.37. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

2.3.1.37.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

2.3.1.37.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

2.3.1.38. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

2.3.1.39. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

2.3.1.40. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

2.3.1.41. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);

2.3.1.42. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

2.3.1.43. Deve possuir módulo para proteção contra port scans, network flooding e MAC spoofing. A base de dados de análise deve ser atualizada juntamente com as vacinas;

2.3.1.44. Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;

2.3.1.45. Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.

2.3.1.46. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.3.1.46.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.3.1.46.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.3.1.47 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

2.3.1.47.1. Discos de armazenamento locais;

2.3.1.47.2. Armazenamento removível;

2.3.1.47.3. Impressoras;

2.3.1.47.4. CD/DVD;

2.3.1.47.5. Modems;

2.3.1.47.6. Dispositivos multifuncionais;

2.3.1.47.7. Leitores de smart card;

2.3.1.47.8. Wi-Fi;

2.3.1.47.9. Adaptadores de rede externos;

2.3.1.47.10. Dispositivos MP3 ou smartphones;

2.3.1.47.11. Dispositivos Bluetooth;

2.3.1.47.12. Câmeras e Scanners.

2.3.1.48. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

2.3.1.49. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

2.3.1.50. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

2.3.1.51. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras.

2.3.1.52. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.

2.3.1.53. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

2.3.1.54. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

2.3.1.55. Ter a capacidade de detectar a modificação de firmware em dispositivos USB mal-intencionado.

2.3.1.56. Deverá realizar a validação dos dispositivos que se conectam via USB que emulam teclados;

2.3.1.57. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

2.3.1.57.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.3.1.57.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.3.1.58. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

2.3.1.59. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

2.3.1.60. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

2.3.1.61. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

2.3.1.62. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

2.3.1.63. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

2.3.1.64. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

2.3.1.65. Capacidade de integração com a Antimalware Scan Interface (AMSI).

2.3.1.66. Deve permitir realizar o gerenciamento por meio de integração via REST API.

2.3.1.67. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.

2.4. Estações Mac OS X

2.4.1. Compatibilidade:

2.4.1.1. macOS Mojave 10.14

2.4.1.2. macOS Catalina 10.15

2.4.1.3. macOS Big Sur 11.0

2.4.1.4. macOS Monterey 12

2.4.2. Características:

2.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;

2.4.2.3. Possuir módulo de bloqueio á ataques na rede;

2.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

2.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;

2.4.2.6. Possibilidade de importar uma chave no pacote de instalação;

2.4.2.7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.4.2.8. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

2.4.2.9. Capacidade de voltar para a base de dados de vacina anterior;

2.4.2.10. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.4.2.11. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

2.4.2.12. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

2.4.2.13. Capacidade de verificar somente arquivos novos e alterados;

2.4.2.14. Capacidade de verificar objetos usando heurística;

2.4.2.15. Capacidade de agendar uma pausa na verificação;

2.4.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.4.2.16.1. Perguntar o que fazer, ou;

2.4.2.16.2. Bloquear acesso ao objeto;

2.4.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.4.2.16.2.2. Caso positivo de desinfecção:

2.4.2.16.2.1. Restaurar o objeto para uso;

2.4.2.16.2.2. Caso negativo de desinfecção:

2.4.2.16.2.3. Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.4.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

2.4.2.18. Capacidade de verificar arquivos de formato de email;

2.4.2.18. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

2.4.2.19.Capacidade de, através da mesma console central de gerenciamento:

2.4.2.19.1. Ser instalado;

2.4.2.19.2. Ser removido;

2.4.2.19.3. Ser gerenciado;

2.5. Sistemas operacionais Linux

2.5.1. Compatibilidade:

2.5.1.1. Plataforma 32-bits:

2.5.1.1.1. Red Hat Linux 6.7 e superior;

2.5.1.1.2. CentOS 6.7 e superior;

2.5.1.1.3. Debian 9.4 e superior;

2.5.1.1.4. Debian 10.1 e superior;

2.5.1.1.5. Debian 11.1 e superior;

2.5.1.1.6. Linux Mint 19 e superior;

2.5.1.1.7. Mageia 4;

2.5.1.2. Plataforma 64-bits:

2.5.1.2.1. Ubuntu 18.04 e superior;

2.5.1.2.2. Ubuntu 20.04;

2.5.1.2.3. Red Hat Enterprise Linux 6.7;

2.5.1.2.4. Red Hat Enterprise Linux 7.2;

2.5.1.2.5. Red Hat Enterprise Linux 8.0;

2.5.1.2.6. CentOS 6.7 e superior;

2.5.1.2.7. CentOS 7.2 e superior;

2.5.1.2.8. CentOS 8.0 e superior;

2.5.1.2.9. Debian 9.4 e superior;

2.5.1.2.10. Debian 10.1 e superior;

2.5.1.2.11. OracleLinux 7.3 e superior;

2.5.1.2.12. OracleLinux 8 e sueperior;

2.5.1.2.13. SUSE Server 12 e superior;

2.5.1.2.14. SUSE Server 15 e superior;

2.5.1.2.15. openSUSE Leap 15;

2.5.1.2.16. Amazon Linux 2;

2.5.1.2.17. Linux Mint 19 e superior;

2.5.1.2.18. Linux Mint 20.1 e superior;

2.5.1.2.19. Oracle Linux 7.3 e superior;

2.5.1.2.20. Oracle Linux 8.0 e superior;

2.5.1.2.21. RED OS 7.2;

2.6. Características:

2.6.1.1. Deve prover as seguintes proteções:

2.6.1.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.6.1.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:

2.6.1.3.1. Via linha de comando;

2.6.1.3.2. Via console administrativa;

2.6.1.3.3. Via GUI;

2.6.1.3.4. Via web (remotamente);

2.6.1.4. Deve possuir funcionalidade de scan de drives removíveis, tais como:

2.6.1.4.1. CDs;

2.6.1.4.2. DVDs;

2.6.1.4.3. Discos blu-ray;

2.6.1.4.4. Flash drives (pen drives);

2.6.1.4.5. HDs externos;

2.6.1.4.6. Disquetes;

2.6.1.5. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:

2.6.1.5.1. Por tipo de dispositivo;

2.6.1.5.2. Por barramento de conexão.

2.6.1.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

2.6.1.7. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.6.1.7.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

2.6.1.7.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

2.6.1.7.3. Leitura de configurações;

2.6.1.7.4. Modificação de configurações;

2.6.1.7.5. Gerenciamento de Backup;

2.6.1.7.6. Visualização de logs;

2.6.1.7.7. Gerenciamento de logs;

2.6.1.7.8. Gerenciamento de ativação da aplicação;

2.6.1.7.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

2.6.1.8. Capacidade de criar exclusões por local, máscara e nome da ameaça;

2.6.1.9. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

2.6.1.10. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

2.6.1.11. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

2.6.1.12. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

2.6.1.12.1. Alta;

2.6.1.12.2. Média;

2.6.1.12.3. Baixa;

2.6.1.12.4. Recomendado;

2.6.1.13. Gerenciamento de backup de arquivos: Fazer backup de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de backup;

2.6.1.14. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

2.6.1.15. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

2.6.1.16. Capacidade de definir o consumo de recursos nas varreduras para não impactar outros aplicativos que necessitem de mais recursos de memória ou processamento;

2.6.1.17. Deverá ser possível priorizar a execução de tarefas;

2.6.1.18. Capacidade de verificar objetos usando heurística;

2.6.1.19. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em malicioso;

2.6.1.20. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP;

2.6.1.21. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

2.6.1.21.1. Detecção de phishing e sites maliciosos;

2.6.1.21.2. Bloqueio de download de arquivos maliciosos;

2.6.1.22.3. Bloqueio de adware;

2.6.1.22.4. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

2.6.1.22. Deve fornecer a possibilidade de administração remota através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux);

2.6.1.23. Deverá fornecer informações de todas as executáveis das aplicações;

2.6.1.24. Deve possuir módulo de proteção contra criptografia maliciosa.

2.6.1.25. Deverá possuir controle de execução de aplicações;

2.6.1.26. O modulo de controle de aplicação deverá possuir as seguintes funcionalidades:

2.6.1.26.1. Criação de lista de bloqueio de aplicação;

2.6.1.26.2. Criação de lista de permissão de aplicação;

2.6.1.27. Deverá realizar busca de ameaças em setores críticos do sistema operacional:

2.6.1.27.1. Setor de inicialização;

2.6.1.27.2. Objetos de inicialização;

2.6.1.27.3. Processos de memória;

2.6.1.27.4. Memória do kernel;

2.7. Compatibilidade com servidores windows;

2.7.1. Compatibilidade de sistema legado:

2.7.2. Plataforma x32 ou x64:

2.7.2.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;

2.7.2.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;

2.7.3. Características:

2.7.3.1. Deve prover as seguintes proteções:

2.7.3.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.7.3.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;

2.7.3.1.3. Firewall com IDS;

2.7.3.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2.7.3.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.7.3.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:

2.7.3.3.1. Via console administrativo;

2.7.3.3.2. Via web (remotamente);

2.7.3.4. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

2.7.3.5. Deverá ter a capacidade de customizar o uso de CPU para realização de scanner no dispositivo.

2.7.3.6. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.7.3.6.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

2.7.3.6.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

2.7.3.6.3. Leitura de configurações;

2.7.3.6.4. Modificação de configurações;

2.7.3.6.5. Gerenciamento de backup;

2.7.3.6.6. Visualização de logs;

2.7.3.6.7. Gerenciamento de logs;

2.7.3.6.8. Gerenciamento de ativação da aplicação;

2.7.3.6.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

2.7.3.6.10. Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.

2.7.3.7. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.7.3.7.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.7.3.7.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

2.7.3.8. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

2.7.3.9. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;

2.7.3.10. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);

2.7.3.11. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

2.7.3.12. Deve possuir funcionalidade de análise personalizada de logs do Windows.

2.7.3.13. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

2.7.3.14. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

2.7.3.15. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

2.7.3.16. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.7.3.17. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.7.3.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

2.7.3.19. Capacidade de verificar somente arquivos novos e alterados;

2.7.3.20. Capacidade de escolher qual tipo de objeto composto será verificada (ex: arquivos comprimidos, arquivos auto descompressores, PST, arquivos compactados por compactadores binários, etc.);

2.7.3.21. Capacidade de verificar objetos usando heurística;

2.7.3.22. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

2.7.3.23. Capacidade de agendar uma pausa na verificação;

2.7.3.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.7.3.24.1. Perguntar o que fazer, ou;

2.7.3.24.2. Bloquear acesso ao objeto;

2.7.3.24.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.7.3.24.2.2. Caso positivo de desinfecção:

2.7.3.24.2.2.1. Restaurar o objeto para uso;

2.7.3.24.2.3. Caso negativo de desinfecção:

2.7.3.24.2.3.1. Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.7.3.25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

2.7.3.26. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos maliciosos em área de backup;

2.7.3.27. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

2.7.3.28. Em caso de detecção de sinais de uma infecção ativa, deve possuir capacidade de, automaticamente:

2.7.3.28.1. Executar os procedimentos pré-configurados pelo administrador;

2.7.3.28.2. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.

2.7.3.29. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

2.7.3.30. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

2.7.3.31. Capacidade de detectar anomalias no comportamento de um software usando análise heurística.

2.7.3.32. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

2.7.3.33. Deve possuir controle de dispositivos externos.

2.8. Smartphones e tablets

2.8.1. Compatibilidade:

2.8.1. Suportar o Android das versões: 5.0 ao 12.

2.8.2. Características:

2.8.2.1. Deve prover as seguintes proteções:

2.8.2.1.1 Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

2.8.2.1.2. Proteção contra adware e autodialers;

2.8.2.1.3. Todos os objetos transmitidos;

2.8.2.1.4. Arquivos abertos no smartphone;

2.8.2.1.5. Programas instalados usando a interface do smartphone

2.8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

2.8.2.2 Deverão isolar em área de backup os arquivos infectados;

2.8.2.3. Deverá atualizar as bases de vacinas de modo agendado;

2.8.2.4. Capacidade de desativar por política:

2.8.2.4.1. Wi-fi;

2.8.2.4.2. Câmera;

2.8.2.4.3. Bluetooth.

2.8.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

2.8.2.6 Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

2.8.2.6. Deverá ter firewall pessoal;

2.8.2.6. Capacidade de tirar fotos quando a senha for inserida incorretamente;

2.8.2.7. Capacidade de enviar comandos remotamente de:

2.8.2.7.1. Localizar;

2.8.2.7.2. Bloquear.

2.8.2.7.3. Capacidade de detectar Root nos dispositivos;

2.8.2.7.4. Capacidade de bloquear o acesso a site por categoria em dispositivos;

2.8.2.7.5. Capacidade de bloquear o acesso a sites phishing ou maliciosos;

2.8.2.7.6. Capacidade de configurar White e blacklist de aplicativos;

2.8.2.7.7. Capacidade de localizar o dispositivo quando necessário;

2.8.2.7.8. Permitir atualização das definições quando estiver em “roaming”;

2.8.2.7.9. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

2.8.2.7.9. Capacidade de agendar uma verificação;

2.8.2.7.10. Capacidade de enviar URL de instalação por e-mail;

2.8.2.7.11. Capacidade de fazer a instalação do agente através de um link QRCode;

2.8.2.7.12. Capacidade de executar as seguintes ações caso a desinfecção falhe:

ü Deletar;

ü Ignorar;

ü Fazer backup;

ü Perguntar ao usuário.

2.8.3. Gerenciamento de dispositivos móveis (MDM) – Android:

2.8.3.1. Compatibilidade:

2.8.3.1.1. Dispositivos com os sistemas operacionais:

2.8.3.1.1.1. Do Android versão 5.0 a 12

2.8.3.1.1.2. Deverá possuir integração com sistemas de gerenciamentos:

2.8.3.1.2.1. VMWare AirWatch 9.3;

2.8.3.1.2.2. MobileIron;

2.8.3.1.2.3. IBM Maas360;

2.8.3.1.2.4. Microsoft Intune;

2.8.3.1.2.5. SOTI MobiControl;

2.8.3.2 Características:

2.8.3.2.1. Capacidade de aplicar políticas de Activesync através do servidor Microsoft Exchange;

2.8.3.2.2. Capacidade de ajustar as configurações de:

2.8.3.2.2.1. Sincronização de e-mail;

2.8.3.2.2.2. Uso de aplicativos;

2.8.3.2.2.3. Senha do usuário;

2.8.3.2.2.4. Criptografia de dados;

2.8.3.2.2.5. Conexão de mídia removível.

2.8.3.2.2.6. Capacidade de instalar certificados digitais em dispositivos móveis;

2.8.3.2.2.7. Deve permitir configurar horário para sincronização do dispositivo com o console de gerenciamento;

2.8.3.2.2.8. Capacidade de desinstalar remotamente o antivírus do dispositivo;

2.8.3.2.2.9. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;

2.8.3.2.2.10 Capacidade de sincronizar com Samsung Knox;

2.8.4. Gerenciamento de dispositivos móveis (MDM) – iOS

2.8.4.1. Compatibilidade:

2.8.4.1.1. Ser compatível com dispositivos com os sistemas operacionais:

2.8.4.1.1.1. iOS 10.0 – 10.3.3

2.8.4.1.1.2. iOS 11.0 – 11.3

2.8.4.1.1.3. iOS 12.0

2.8.4.1.1.4. iOS 13.0

2.8.4.1.1.5. IPadOS 13 ao 15

2.8.4.1.2 Características:

2.8.4.1.2.1. Capacidade de aplicar políticas de Activesync através do servidor Microsoft Exchange;

2.8.4.1.3. Capacidade de ajustar as configurações de:

2.8.4.1.3.1. Sincronização de e-mail;

2.8.4.1.3.2 Senha do usuário;

2.8.4.1.3.3 Criptografia de dados;

2.8.4.1.3.4 Capacidade de instalar certificados digitais em dispositivos móveis;

2.8.4.1.3.5 Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos clientes através de:

2.8.4.1.3.5.1. Link por e-mail;

2.8.4.1.3.5 .2 Link por mensagem de texto;

2.8.4.1.3.5.3 QR Code

2.8.4.1.3.6 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

2.8.4.1.3.7 Capacidade de, remotamente, bloquear um dispositivo iOS;

2.9 Criptografia

2.9.1. Compatibilidade:

2.9.1.2. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;

2.9.1.3. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;

2.9.1.4. Microsoft Windows 7 Professional SP1 ou superior x86/x64;

2.9.1.5. Microsoft Windows 8 Enterprise x86/x64;

2.9.1.6. Microsoft Windows 8 Pro x86/x64;

2.9.1.7. Microsoft Windows 8.1 Pro x86/x64;

2.9.1.8. Microsoft Windows 8.1 Enterprise x86/x64;

2.9.1.9. Microsoft Windows 10 Enterprise x86/x64;

2.9.1.10. Microsoft Windows 10 Pro x86/x64;

2.9.2. Características:

2.9.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

2.9.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

2.9.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

2.9.2.4. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;

2.9.2.5. Permitir criar vários usuários de autenticação pré-boot;

2.9.2.6. Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real;

2.9.2.7. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

2.9.2.8. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

2.9.2.9. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

2.9.2.10. Criptografar todos os arquivos individualmente;

2.9.2.11. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

2.9.2.12. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

2.9.2.13. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente;

2.9.2.14. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

2.9.3. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

2.9.4. Verifica compatibilidade de hardware antes de aplicar a criptografia;

2.9.5. Possibilita estabelecer parâmetros para a senha de criptografia;

2.9.6. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

2.9.7. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo;

2.9.8. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

2.9.9 Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

2.9.10. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;

2.9.11. Permite criar um grupo de extensões de arquivos a serem criptografados;

2.9.12. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

2.9.13. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

2.9.14. Capacidade de deletar arquivos de forma segura após a criptografia;

2.9.15. Capacidade de criptografar somente o espaço em disco utilizado;

2.9.16. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

2.9.17. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

2.9.18. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;

2.9.19. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

2.9.20. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

2.9.21. Capacidade de fazer “Hardware encryption”;

2.10. Gerenciamento de Sistemas

2.10.1.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;

2.10.1.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

2.10.1.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

2.10.1.4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

2.10.1.5. Capacidade de gerenciar licenças de softwares de terceiros;

2.10.1.6. Capacidade de atualizar informações sobre hardware presentes nos relatórios após mudanças de hardware nas máquinas gerenciadas;

2.10.1.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc);

2.10.2 Possibilita fazer distribuição de software de forma manual e agendada;

2.10.3 Suporta modo de instalação silenciosa;

2.10.4 Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

2.10.1.5 Possibilita fazer a distribuição através de agentes de atualização;

2.10.1.6 Utiliza tecnologia multicast para evitar tráfego na rede;

2.10.1.7 Possibilita criar um inventário centralizado de imagens;

2.10.1.8. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

2.10.1.9. Suporte a WakeOnLan para deploy de imagens;

2.10.1.10. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

2.10.1.11. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

2.10.1.12 Capacidade de gerar relatórios de vulnerabilidades e patches;

2.10.1.13 Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

2.10.1.14 Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

2.10.1.15 Permite baixar atualizações para o computador sem efetuar a instalação;

2.10.1.16 Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

2.10.1.17 Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

2.10.1.18 Permite selecionar produtos a serem atualizados pela console de gerenciamento;

2.10.1.18 Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;

2.10.1.19 Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

2.10.1.20 Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

2.10.1.21 Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;

2.10.1.22 Deve permitir selecionar o idioma das aplicações que serão atualizadas;

2.10.1.23 Permitir agendar o sincronismo entre o console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

2.11 Detecção e Resposta

2.11.1. Compatibilidade:

2.11.1.1 Deve ser compatível com os seguintes sistemas de estação de trabalho:

2.11.1.1.1 Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

2.11.1.1.2 Microsoft Windows 8 Professional/Enterprise;

2.11.1.1.3 Microsoft Windows 8.1 Professional / Enterprise;

2.11.1.1.4 Microsoft Windows 10 Pro / Enterprise / Home / Education;

2.11.1.1.5 Microsoft Windows 11 Pro / Enterprise / Home / Education;

2.11.1.1.6 Deve ser compatível com os seguintes sistemas servidores:

2.11.1.1.6.1 Windows Small Business Server 2011 Essentials / Standard (64-bit)

2.11.1.1.6.2. Windows MultiPoint Server 2011 (64-bit);

2.11.1.1.6.3. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

2.11.1.1.6.4. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

2.11.1.1.6.5. Windows Server 2016 Essentials / Standard / Datacenter;

2.11.1.1.6.6. Windows Server 2019 Essentials / Standard / Datacenter;

2.11.1.1.6.7. Windows Server 2022.

2.11.2. Características

2.11.2.1 As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;

2.11.2.2 A solução deve oferecer módulo focado em capacidades de EDR “Endpoint Detection and Response”, incluindo no mínimo as seguintes capacidades:

2.11.2.3 O agente deve ter capacidade de coletar e processar dados relacionados ao veredito e ao contexto da ameaça;

2.11.2.4 Deve fornecer graficamente a visualização da cadeia do ataque;

2.11.2.5 Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).

2.11.3. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

2.11.3.1. Isolar o host;

2.11.3.2. Iniciar uma varredura nas áreas críticas;

2.11.3.3. Quarentenar o objeto;

2.11.4 A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

2.11.5 Visibilidade das detecções provenientes de endpoint;

2.11.5.1. Processos;

2.11.5.2. Conexões remotas;

2.11.5.3 Alterações de registros;

2.11.5.4 Objetos baixados

2.11.6 Capacidade de integração com a solução de sandbox cloud do fabricante;

2.11.7 Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.

2.11.8 Deverá possuir informações de assinaturas digitais da ameaça;

2.11.9 Deve ser capaz de trazer informações do arquivo sobre sua geolocalização;

2.11.10 Possibilidade de informar quando o arquivo foi detectado pela base de conhecimento;

2.11.11 Trazer a identificação de comportamento e/ou descrição sobre o arquivo;

2.11.12 A solução deve oferecer no mínimo as seguintes opções de resposta:

2.11.12.1 Prevenir a execução de um arquivo;

2.11.12.2. Quarentenar um arquivo;

2.11.12.3. Iniciar uma varredura por IoC;

2.11.12.4. Parar um processo;

2.11.12.5. Executar um processo;

2.11.13 Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

2.11.13.1 A opção de isolamento deve estar disponível junto a visualização do incidente;

2.11.13.2 Na analise do incidente a ferramenta deverá apresentar recomendações de ações que o analista precisa executar para remediar o incidente;

2.11.13.3 As recomendações devem ser guiadas juntamente com guias das opções selecionadas pelo analista, apresentando pop-up guiando as ações.

2.11.13.4 Deverá ser possível remover a máquina do isolamento a partir do incidente;

2.11.13.5 Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

2.11.13.6 Deve oferecer informações de inteligência de ameaças do próprio fabricante;

2.11.13.7 Deverá possuir detecção baseada em sandbox do tipo cloud;

2.11.13. 8 Deverá suportar IoC de terceiros em formatos OpenIOC.

1.3.3.2 Requisitos de Capacitação:

Não se prevê a necessidade de treinamento formal para usuários finais, a equipe técnica da Coordenadoria de TIC do Tribunal já possui expertise comprovada na operação, gestão e suporte da solução Kaspersky, o que proporciona:

· Redução de curva de aprendizado;

· Evitação de cursos de capacitação adicionais, que impactariam o orçamento e o cronograma institucional;

· Melhoria na qualidade do suporte interno, com respostas mais rápidas e eficientes em situações críticas.

1.3.3.3 Requisitos de Manutenção:

O fornecedor deve oferecer suporte técnico especializado, disponível para auxiliar na resolução de problemas, manutenção preventiva e atualizações. O suporte deve estar disponível em regime 24/7 para garantir a prontidão na resposta a incidentes críticos.

A contratada deverá disponibilizar equipe de suporte técnico qualificada para atendimento durante todo o período de vigência contratual, garantindo a correta implantação, atualização e manutenção da solução.

O suporte deverá abranger tanto a camada de infraestrutura em nuvem quanto à integração com o ambiente corporativo do TJM/RS, incluindo políticas de autenticação, conectividade segura e proteção contra ameaças avançadas.

O serviço de atendimento de 1º nível aos administradores dos clientes e suporte técnico deverá ser prestado através da Central de Atendimento (Help-Desk) da Contratada, conforme os canais oficiais disponibilizados pela empresa contratada, como: 0800 – e-mail, observando-se as condições e níveis de serviço especificados pelo fabricante Kaspersky.

- Os prazos de atendimento sem qualquer ônus para Administração serão os seguintes:

1 normal: no máximo 2 (dois) dias corridos, a contar da data e hora de abertura do chamado;

2 urgente: no máximo 4 (quatro) horas corridas a contar da data e hora de abertura do chamado;

- os atendimentos serão prestados nas dependências do Tribunal de Justiça Militar do Rio Grande do Sul, em Porto Alegre, RS, desde que a instalação e o suporte Técnico não possa se dar via acesso remoto.

Entende-se por horário comercial o compreendido entre 08:00hs e 18:00hs, de segundas à sextas- feiras, exceto em feriados.

1.3.3.4. Requisitos de Implantação:

A contratada deverá durante o processo inicial de implantação, a equipe da contratada deverá acompanhar a configuração e ativação das licenças, garantindo o alinhamento às políticas de segurança da instituição. O plano deverá prever fases de teste, homologação e entrada em produção, com registro formal das atividades executadas e responsáveis designados.

Toda a implantação deverá ocorrer sem prejuízo às atividades institucionais do Tribunal, garantindo plena operação dos serviços a partir do primeiro dia útil após a instalação.

A execução do contrato deverá ser formalmente iniciada mediante a emissão de ordem de fornecimento ou documento equivalente, a ser assinado pela Administração, com a finalidade de registrar o início da entrega, instalação e ativação dos equipamentos, bem como a disponibilização do software de bilhetagem e suporte técnico. Esse procedimento é essencial para controle da execução contratual, marcação do início das obrigações da contratada e registro de aceite institucional, promovendo maior transparência, rastreabilidade e segurança jurídica.

1.3.3.5. Requisitos de experiência profissional:

A equipe técnica da contratada responsável pela execução dos serviços deverá possuir experiência comprovada na instalação, manutenção

e gerenciamento**,** com apresentação de atestados de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, compatíveis com o objeto licitado. A comprovação poderá se dar por meio de contratos anteriores, declarações de capacidade técnica ou registros formais de atuação.

1.3.3.6. Requisitos de formação da equipe:

A equipe técnica responsável pela instalação da solução deverá possuir certificações ou comprovação de experiência em soluções de segurança cibernética, preferencialmente relacionadas à plataforma Kaspersky Next EDR Optimum com gerenciamento à gestão de ambientes em nuvem.

Será exigida a comprovação de treinamentos prévios ou a disponibilização de capacitação oficial, ministrada pelo fabricante ou parceiro homologado, abrangendo os módulos de gerenciamento centralizado, resposta a incidentes e configuração de políticas de segurança.

1.3.3.7. Requisitos Temporais:

O software Kaspersky é executado nas máquinas da contratante, sendo que a contratada deverá disponibilizar o serviço durante as 24 (vinte e quatro) horas diárias, nos 7 (sete) dias da semana, ressalvadas as paradas para manutenção ou instalação de equipamentos da contratada, que deverão ser previamente comunicadas à Coordenadoria de Tecnologia da Informação e Comunicação - TIC, por meio do telefone (51) 3214-1074 ou e-mail "Coordenadoria de TIC" ou "Eduardo Severo" (eduardo@tjmrs.jus.br). Substituindo o texto anteriormente informado como gestão de banco de dados para software Kaspersky.

SLA, escopo e Disponibilidade do Suporte: O suporte deve garantir alta disponibilidade e resposta rápida a incidentes. O modelo proposto de abertura de chamados com primeira resposta em oito horas úteis e apenas suporte nível 1 não atende plenamente às necessidades da contratante, sendo exigida maior abrangência no suporte técnico, incluindo níveis mais avançados de atendimento. Serviço de atendimento de 1º nível aos administradores dos clientes e suporte técnico deverá ser prestado, conforme os canais oficiais disponibilizados pela empresa contratada, através de canais como: Central de Atendimento (Help-Desk), 0800 – e-mail, observando-se as condições e níveis de serviço especificados pelo fabricante Kaspersky.

Os serviços a serem prestados abrangerão todas as instalações do TJMRS Porto Alegre:

1- Sede: Av Praia de Belas, 799, Bairro Praia de Belas, Centro Histórico, Porto Alegre, RS; (51) 3214-1000

2 - 1ª Auditoria - Av Praia de Belas, 799, Bairro Praia de Belas, Centro Histórico, Porto Alegre, RS; (51) 3214-1060

3 - 2ª Auditoria - Av Praia de Belas, 799, Bairro Praia de Belas, Centro Histórico, Porto Alegre, RS; Fone (51)3214-1032

4 – 3ª Auditoria de Santa Maria- Av Nossa Sra. Das Dores, 437, Santa Maria, RS – CEP 97050-531;Fone (55)3223-1287

5 – 4ª Auditoria de Passo Fundo – Rua Cel. Pelegrini, 700, Bairro Cruzeiro/Rodrigues, Passo Fundo - CEP 99070-010, RS; (55)3311-4699.

Prazo de entrega: 02 dias após publicação da súmula do contrato;

A contagem de prazo poderá ser suspensa durante o período de recesso (final do ano);

Os serviços a serem prestados deverão ser entregue no TJMRS Porto Alegre, Av Praia de Belas, 799, Bairro Praia de Belas, Centro Histórico, Porto Alegre, RS, à Coordenadoria de Tecnologia da Informação e da Comunicação-TIC e-mail "Coordenadoria de TIC" ou "Eduardo Severo" (eduardo@tjmrs.jus.br) telefone (51) 3214-1074.

1.3.3.8. Requisitos de Segurança da Informação

A CONTRATADA deverá seguir os procedimentos básicos mínimos de segurança listados:

a) Observar, rigorosamente, todas as normas e procedimentos de segurança aplicados no ambiente de Tecnologia da Informação do CONTRATANTE, inclusive sua Política de Segurança da Informação e Comunicações – quando aplicável ao objeto;

b) A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do CONTRATANTE;

c) No que couber, a solução deve contemplar possuir garantia mínima de disponibilidade; proteção contra vazamento de dados e fraudes digitais e, quando aplicável, garantir a segurança dos arquivos armazenados em nuvem.

O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD /ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Decreto nº 11.462, de 31 de março de 2023, e a outras legislações aplicáveis.

1.3.3.9. Requisitos Sociais, Ambientais e Culturais:

A solução contratada deverá observar os princípios da sustentabilidade definidos no Plano de Logística Sustentável (PLS) do TJMRS, bem como as diretrizes da Resolução CNJ nº 400/2021, que institui a política de sustentabilidade no âmbito do Poder Judiciário. Ainda que a natureza do serviço não envolva produtos de consumo direto, a contratada deverá adotar práticas responsáveis, tais como a destinação adequada de resíduos (toners e peças substituídas), a priorização de insumos recicláveis, e o uso de equipamentos com certificações ambientais (como Energy Star ou similares).

· Adotar práticas de responsabilidade social, assegurando que não haja utilização de mão de obra infantil, forçada ou análoga à escravidão;
· Respeitar e promover políticas de diversidade, inclusão e igualdade de oportunidades no quadro de pessoal envolvido na execução do contrato.
· Cumprir integralmente as obrigações trabalhistas, previdenciárias e de segurança e saúde no trabalho, em conformidade com a legislação vigente.

A contratada também deverá estar ciente das Orientações do Controle Interno e dos procedimentos administrativos vigentes no TJMRS, assumindo compromisso com condutas éticas e compatíveis com a cultura institucional do órgão.

1.3.3.10. Requisitos Legais

O presente processo de contratação, visando à aquisição de licença da solução de antivírusKaspersky Next EDR Optimum, com gerenciamento incluso, por meio de adesão à Ata de Registro de Preços, deverá observar integralmente o disposto na Constituição Federal e na legislação infraconstitucional pertinente, em especial:

1. Lei nº 14.133, de 1º de abril de 2021 (Lei de Licitações e Contratos Administrativos), com observância dos princípios da legalidade, impessoalidade, moralidade, publicidade, eficiência, economicidade, transparência, vinculação ao instrumento convocatório e julgamento objetivo;

2. Instrução Normativa SGD/ME nº 94, de 2022, que dispõe sobre as diretrizes para contratações de soluções de tecnologia da informação e comunicação no âmbito da Administração Pública Federal;

3. Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, que regulamenta o uso do procedimento de Ata de Registro de Preços no âmbito da Administração Pública;

4. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), no que couber, especialmente quanto à proteção, integridade, confidencialidade e segurança das informações e dados pessoais processados ou armazenados pela solução contratada;

5. Decreto nº 11.462, de 31 de março de 2023, que dispõe sobre a governança de contratações de soluções de tecnologia da informação e comunicação na Administração Pública Federal;

6. Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI), no que tange à garantia da segurança física e lógica de dados e informações, inclusive em meio impresso, mesmo que não haja tratamento direto de conteúdo documental pela contratada;

7 . Demais normativos e regulamentos específicos aplicáveis à contratação de soluções de segurança cibernética e licenciamento de software no âmbito da Administração Pública.

8. Segurança e Conectividade

A solução a ser contratada deverá:

1 . Garantir proteção de alto nível contra ameaças cibernéticas, abrangendo malwares, ransomwares, phishing e ameaças persistentes avançadas (APTs), com detecção e resposta automatizadas;

2 . Disponibilizar painel central de gerenciamento seguro, com autenticação multifator, controle de permissões baseado em perfis e registro de logs para fins de auditoria e conformidade;

3. Assegurar conectividade criptografada entre os dispositivos protegidos e a controladora da solução, utilizando protocolos seguros (TLS 1.2 ou superior), preservando a integridade e a confidencialidade dos dados;

4. Permitir integração com outras ferramentas corporativas de segurança e gestão, assegurando interoperabilidade e continuidade da proteção no ambiente de TI do TJM/RS.

O cumprimento integral dessas disposições visa assegurar que a contratação seja conduzida dentro dos parâmetros legais, garantindo a proteção dos interesses da Administração Pública, a mitigação de riscos de segurança da informação e a observância das melhores práticas em governança e gestão de contratos de tecnologia da informação.

1.3.3.11. Demais Requisitos Aplicáveis

· Contratada deverá garantir prazo máximo de entrega e instalação de até 05 (trinta) dias úteis, contados da ordem de fornecimento, sob pena de aplicação de penalidades previstas contratualmente.
· A prestação dos serviços poderá ocorrer em regime híbrido, conforme a necessidade operacional, respeitando os protocolos de segurança do TJMRS.
· A contratada deverá cumprir integralmente as obrigações trabalhistas, previdenciárias e de segurança e saúde no trabalho, em conformidade com a legislação vigente.
· A contratada compromete-se a promover o imediato afastamento (em até 24 horas) de qualquer profissional cuja conduta prejudique a fiscalização contratual ou comprometa a confiança da Administração.
· A contratada deverá garantir padrões mínimos de qualidade, rastreabilidade e documentação técnica, assegurando a geração eficiente dos relatórios e o bom desempenho da solução contratada.

1.3.4. Aderência a padrões e modelos

A presente contratação não demanda aderência obrigatória a frameworks, metodologias ou modelos internacionais específicos de governança ou desenvolvimento (como ITIL, COBIT, CMMI ou PMBOK), em razão da natureza operacional da solução. Contudo, recomenda-se que os procedimentos de manutenção, suporte e atendimento técnico estejam alinhados a boas práticas de gestão de serviços, assegurando agilidade, rastreabilidade e controle na execução contratual.

1.3.4.1. Modelo Nacional de Interoperabilidade – MNI

O Modelo Nacional de Interoperabilidade (MNI) é o padrão de comunicação estabelecido pelo Conselho Nacional de Justiça (CNJ) para ser utilizado pelos Tribunais, além de outros órgãos, como o Ministério Público e a Advocacia-Geral da União.

O MNI permite que as informações necessárias ao trâmite eletrônico do processo sejam interpretadas em todos os órgãos da justiça que o utilizam, por meio da padronização da terminologia utilizada na identificação de documentos.

Portando, não se aplica ao contexto deste estudo, uma vez que a demanda está relacionada à contratação de empresa para aquisição de licença da solução de antivírus Kaspersky Next EDR Optimum com gerenciamento não contempla a contratação de solução para intercâmbio de informações de processos judiciais e assemelhados ou servir de base para funcionalidades pertinentes no âmbito do sistema processual conforme definido pela Resolução Conjunta nº 3, de 16 de abril de 2013.

1.3.4.2. Infraestrutura de Chaves Públicas Brasileiras – ICP-Brasil

A contratação da solução de antivírus Kaspersky Next EDR Optimum com gerenciamento deverá observar os princípios de segurança, integridade e validade jurídica das transações eletrônicas, em conformidade com a Infraestrutura de Chaves Públicas Brasileiras – ICP-Brasil, instituída pela Medida Provisória nº 2.200-2/2001.

Considerando que a solução contratada será disponibilizada em ambiente de nuvem (cloud) e que o gerenciamento centralizado de endpoints e incidentes de segurança envolverá a emissão, a validação e o tráfego de informações digitais críticas tornam-se imprescindível que:

1. Certificados Digitais ICP-Brasil sejam utilizados para garantir a autenticidade, integridade e validade jurídica de documentos eletrônicos e registros relacionados à contratação, auditorias e logs de segurança.

2. Toda a comunicação eletrônica entre a contratada e o órgão contratante seja realizada de forma segura, com mecanismos

criptográficos compatíveis com os padrões técnicos da ICP-Brasil, de modo a prevenir adulterações ou interceptações indevidas.

3. O gerenciamento da solução de antivírus em nuvem contemple mecanismos de autenticação robusta (incluindo certificados digitais) para o acesso administrativo, assegurando que somente usuários devidamente autorizados tenham permissão de operação.

4. A assinatura digital de documentos relacionados à contratação, tais como relatórios de monitoramento, evidências de incidentes, atas técnicas e termos de aceite, seja realizada com certificados digitais emitidos no âmbito da ICP-Brasil, garantindo a sua plena validade jurídica perante a legislação brasileira.

5. O fornecedor contratado se comprometa a manter conformidade com a Lei nº 14.133/2021 (Nova Lei de Licitações e Contratos Administrativos), com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) e com a Medida Provisória nº 2.200-2/2001, adotando medidas de governança em segurança da informação que assegurem a rastreabilidade e confiabilidade do serviço prestado.

Dessa forma, a aplicação da ICP-Brasil na presente contratação garante não apenas a conformidade legal e normativa, mas também reforça a segurança jurídica, tecnológica e operacional da solução, em alinhamento com os princípios de eficiência, economicidade e continuidade dos serviços públicos, previstos na Constituição Federal e na legislação vigente.

1.3.4.3. Modelo de Requisitos MoReq-Jus

O Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (MoReq-Jus) é aplicável à contratação para aquisição de licenças da solução Kaspersky Next EDR Optimum com gerenciamento, especialmente considerando a natureza sensível dos dados protegidos por soluções de segurança cibernética e os requisitos de gestão de documentos e registros que este modelo preconiza. Abaixo detalho como isso se aplica e quais considerações são importantes:

1.3.4.3. 1. Gestão de Documentos e Registros:

O MoReq-Jus estabelece requisitos para a gestão de documentos e registros, incluindo metadados, classificações, e controles de acesso. No contexto da aquisição de uma solução como a Kaspersky Next EDR Optimum com gerenciamento, isso implica a necessidade de documentar todo o processo de contratação, licenciamento e implementação, assegurando que os registros sejam autênticos,

1.3.4.3. 2. Licenciamento e Conformidade:

O modelo MoReq-Jus enfatiza a conformidade com políticas de gestão de documentos. No caso do licenciamento da Kaspersky, é crucial documentar os termos da licença, como o tipo de licença (por exemplo, Add-on MDR, EDR Optimum, ou [EDR Optimum+MDR]), o número de dispositivos cobertos, e os métodos de ativação (via chave ou arquivo BLOB). Isso garante que a organização possa comprovar conformidade com as políticas internas e externas.

1.3.4.3. 3. Preservação e Auditoria:

O MoReq-Jus requer que sistemas de gestão de documentos permitam auditoria e preservação de registros. Para a solução Kaspersky, isso significa que logs de detecção de ameaças, registros de incidentes, e metadados de licenças devem ser armazenados de forma segura e acessível para auditorias, alinhando-se com requisitos de segurança e compliance.

1.3.4.3. 4. Metadados e Classificação:

O modelo exige a uso de metadados para classificação e recuperação de documentos. Na aquisição da Kaspersky, metadados relacionados às licenças (como datas de expiração, número de dispositivos, e tipos de soluções) devem ser catalogados no sistema de gestão de documentos da organização, facilitando a gestão do ciclo de vida da licença e a renovação contratual.

1.3.4.3. 5. Acesso e Segurança:

O MoReq-Jus define controles de acesso para documentos sensíveis. Como a solução Kaspersky lida com dados críticos de segurança, é

essencial garantir que apenas pessoal autorizado tenha acesso às informações de licenciamento e gestão da solução, alinhando-se com os princípios de confidencialidade e integridade do modelo.

1.3.4.3. 6. Considerações Adicionais

Aquisição de Licenças: A aquisição da licença deve considerar a quantidade mínima de dispositivos exigida pela Kaspersky, conforme detalhado nos resultados de busca. Por exemplo, licenças comerciais podem exigir um mínimo de 200 dispositivos, o que deve ser documentado no processo de contratação.

Implementação Técnica: A implementação da solução deve seguir os métodos de licenciamento suportados, como a uso de chaves únicas ou arquivos BLOB, assegurando que a gestão desses elementos esteja alinhada com os requisitos de rastreabilidade do MoReq-Jus

A aplicação do MoReq-Jus assegura que a contratação para aquisição da solução Kaspersky Next EDR Optimum com gerenciamento seja realizada de forma estruturada, auditável e em conformidade com os requisitos de gestão de documentos e registros. Isso é particularmente relevante para organizações que lidam com dados sensíveis e necessitam de robustos controles de governance e compliance.

1.4 Atendimento da demanda

1.4. Atendimento da demanda

1.4.1. Portal do Software Público Brasileiro

O Portal do Software Público Brasileiro consolida-se como uma iniciativa que conseguiu criar um ambiente comum para compartilhar soluções de software no setor público, racionalizar a gestão dos recursos de informática, reaproveitar as soluções de software existentes para diminuir custos e atividades redundantes, estabelecer parcerias e ações cooperadas e reforçar a política pública de estimular o uso de software livre.

Contudo, dada à natureza da demanda, não existem soluções de software no Portal do Software Público Brasileiro capaz de satisfazer às necessidades desta contratação, devido ao baixo número de equipamentos necessários para atender a demanda deste Tribunal.

1.4.2. Soluções de TIC

Para a necessidade apontada, foram identificadas diversas outras empresas oferecem soluções de EDR (Endpoint Detection and Response) no mercado. Com base nos resultados de busca e no conhecimento geral do setor, aqui estão algumas das principais alternativas, incluindo informações técnicas, valores estimados e comparações:

1.4.2.1. Solução 1: Microsoft Defender for Edenpoint

Poteção avançada contra ameaças, investigação de incidentes e resposta automatizada. Inclui proteção em tempo real, análise de comportamento e integração com o Azure Sentinel .

· Valores Estimados:

- Preço por endpoint/ano: R$ 495,72- R$ 5.948,64 (dependendo do volume e licenciamento Enterprise).
- Memória de Cálculo para 250 endpoints:
  - § 250 × R$ 5.948,64 = R$ 1.487.160,00/ano.

· Comparação:

- Vantagens: Integração nativa com Windows e Office 365, ideal para ambientes Microsoft.
- Desvantagens: Pode requerer configuração adicional para ambientes heterogêneos (Linux/macOS).

1.4.2.2. Solução 2: CrowdStrike Falcon Insight

Definição Técnica: Plataforma EDR baseada em nuvem, com detecção de ameaças em tempo real, caça proativa a ameaças e resposta automatizada. Utiliza IA para análise comportamental.

Valores Estimados:

- Preço por endpoint/ano: R$ 1.735,00 - R$ 20.820,00
- Memória de Cálculo para 250 endpoints:

§ 250 × R$ 20.820,00 = R$ 26.025.000,00/ano.

Comparação:

- Vantagens: Alta escalabilidade e baixo impacto no desempenho dos endpoints.
- Desvantagens: Custos mais elevados em comparação com soluções básicas.

1.4.2.3. Solução 3: Kaspersky Next EDR Optimum

Definição Técnica: Solução EDR autônoma com proteção preventiva, detecção de ameaças e resposta automatizada. Inclui recursos de IA e análise de comportamento. Projetada segurança abrangente que combina proteção de endpoints com funcionalidades de EDR para ajudar empresas a enfrentar ameaças complexas de forma eficiente e econômica.

Valores Estimados:

- Preço por endpoint/ano: R$ 794,50 - R$ 5.517,36
- Memória de Cálculo para 250 endpoints:

§ 250 × R$ 66.208,33 × 3= R$ 198.625,00/36 .

Comparação:

- Vantagens: oferece segurança avançada com recursos como detecção e resposta a ameaças, automação e visibilidade em endpoints, mas pode exigir mais conhecimento técnico para configuração e gerenciamento em comparação com a versão Foundations. .
- Desvantagens: Pode requerer mais recursos técnicos para configuração avançada.

1.4.2.4. Solução 4: Trend Micro Vision One

Definição Técnica: Plataforma XDR (Extended Detection and Response) que combina EDR com proteção de e-mail, rede e nuvem. Oferece visibilidade unificada e resposta integrada.

Valores Estimados:

- Preço por endpoint/ano: R$ 325,00 - R$ 3.900,00.
- Memória de Cálculo para 250 endpoints:

§ 250 × R$ 3.900,00 = R$ 975.000,00/ano.

Comparação:

- Vantagens: Escopo ampliado (XDR) com integração multi-camada.
- Desvantagens: Complexidade inicial na implementação.

Comparativo Técnico e Econômico

Solução	Preço/Endpoint/Ano (R$)	Recursos Principais	Integração com SIEM	Conformidade MoReq-Jus
Kaspersky Next EDR Optimum	794,50	EDR completo, segurança na nuvem, gestão de patches.	Sim	Alta
Microsoft Defender	495,72	Integração nativa com Windows, Azure Sentinel	Sim	Moderada
CrowdStrike Falcon	1.735,00	IA avançado, baixo impacto no desempenho.	Sim	Alta
Trend Micro Vision One	325,00	XDR unificado, proteção multi-camada	Sim	Moderada

Recomendações

Kaspersky Next EDR Optimum destaca-se pela relação custo-benefício, recursos de conformidade (como auditoria e metadados para MoReq-Jus) e promoção vigente (36 meses) .

Soluções Alternativas: Microsoft Defender é ideal para ambiente Microsoft, enquanto CrowdStrike oferece IA avançada para ambientes complexos. Trend Micro Vision One é recomendado para organizações que buscam escopo XDR ampliado.

Para Contratação via Ata: A aquisição do Kaspersky via Ata de Registro de Preços é vantajosa devido à agilidade, conformidade com modelos de gestão documental e economia de recursos.

- Tabela Comparativa de Funcionalidades entre Soluções de Segurança

A tabela abaixo compara as funcionalidades técnicas essenciais para uma avaliação objetiva.

Funcionalidade	Kaspersky Next EDR Optimum	Norton 360 Advanced	McAfee Endpoint Security	Avast Business Security	Microsoft Defender for Endpoint	CrowdStrike Falcon	SentinelOne Singularity	Trend Micro Vision One	ESET PROTECT Advanced
Proteção Contra Malware	(99.99% detecção)	(99.8% detecção)	(99.5% detecção)	(Heurística e cloud)	(Nativo Windows)	(IA avançada)	(IA autônoma)	(Proteção multi-camada)	(Proativa)
EDR Avançado	(Análise de causa raiz, resposta guiada)	(Recursos básicos)	(Prevenção básica)	(Focado em antivírus)	(Integrado com XDR)	(Resposta automatizada)	(Resposta autônoma)	(XDR unificado)	(Detecção comportamental)
Gestão de Vulnerabilidades/Patches	(Automatizado	(Software Updater)	(Scan de vulnerabilidades)	(Limitado)	(Integrado com Microsoft 365)	(Gerenciamento de riscos)	(Correção proativa)	(Gestão centralizada)	(Scan de vulnerabilidades)
Conformidade (LGPD, MoReq-Jus)	(Auditoria, metadados)	(Relatórios auditáveis)	(Proteção de dados)	(Básico)	(Integração com Azure)	(Relatórios personalizáveis)	(Logs detalhados)	(Conformidade regulatória)	(Políticas personalizáveis)
Integração com SIEM	(Suporte nativo)	(Não mencionado)	(Via conectores)	(Não suportado)	(Nativo com Azure Sentinel)	(API aberta)	(Integração ampla)	(Correlação multi-fonte)	(Suporte a SIEM)
Segurança em Nuvem	(Monitoramento e bloqueio)	(Backup em nuvem)	(Proteção de dados)	(Limitado a VPN)	(Proteção nativa Azure)	(Proteção de workloads)	(Segurança de containers)	(Proteção multi-cloud)	(Proteção de cloud)
VPN Incluído	(300 MB/dia)	(Ilimitado)	(Não incluído)	(Apenas planos premium)	(Não incluído)	(Add-on separado)	(Não incluído)	(Não incluído)	(Não incluído)
Impacto no Desempenho	(Baixo consumo)	(Alto durante varreduras)	(Moderado)	(Alto em memória)	(Otimizado para Windows)	(Arquitetura leve)	(Baixa latência)	(Moderado)	(Leve)

Funcionalidade	Kaspersky Next EDR Optimum	Norton 360 Advanced	McAfee Endpoint Security	Avast Business Security	Microsoft Defender for Endpoint	CrowdStrike Falcon	SentinelOne Singularity	Trend Micro Vision One	ESET PROTECT Advanced
Suporte a Modelos de Ameaça (MITRE ATT&CK)	(Parcial)	(Não mencionado)	(Não mencionado)	(Não mencionado)	(Integrado)	(Mapeamento completo)	(Mapeamento nativo)	(Suporte avançado)	(Limitado)

1.4.3. Contratações Públicas Similares:

Os seguintes órgãos realizaram contratações cujo objeto apresenta similaridade quanto às alternativas de solução propostos neste estudo preliminar.

1.4.3.1. Órgão 1 - Prefeitura Municipal de Araucária – PR

Unidade compradora**:** UASG 925532

Disponível em Link

<https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=92553205900912024>

Pregão Eletrônico N° 90091/2024

Objeto da contratação: "Software" Aplicação: Informática, Tipo: Client Server Suite , Características Adicionais: Antivírus Corporativo, Atualização Contínua E Su-

Fonte: Compras.gov.br

Demais itens registrados no edital em menção não atendem as necessidades e requisitos técnicos necessários para a escolha como similar.

1.4.3.2. Órgão 2 - Câmara Municipal de Belo Horizonte

Unidade compradora: UASG 926306

Disponível em Link

<https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=92630605900302024>

Pregão Eletrônico nº 90030/2024

Objeto da contratação: Licenciamento de solução centralizada de segurança do tipo endpoint protection por 36 (trinta e seis) meses, incluindo a sua implantação, repasse de conhecimento e direito a suporte técnico.

Fonte: Compras.gov.br

1.4.3.3. Órgão 3 - Itabirito Câmara Municipal

Unidade compradora: 930116 - Câmara Municipal de Itabirito - MG

Disponível em Link < https://pncp.gov.br/app/editais/18366963000179/2025/78>

Contratação Direta nº 90029/2025

Id contratação PNCP: 18366963000179-1-000078/202

Objeto da contratação Licença Software Antivírus

Fonte: Compras.gov.br

1.4.4. Soluções similares em outros órgãos

No levantamento realizado junto a bases de dados públicas e sistemas oficiais de contratações (como ComprasNet, PNCP e atas vigentes), não foram identificadas contratações de soluções substancialmente distintas ou alternativas que possam atender às necessidades desta demanda com nível equivalente de desempenho e segurança diferentes às citadas no item 1.4.2 deste ETP.

1.4.5. Modelos de Aquisição/Prestação do Serviço

Para o Tribunal de Justiça Militar do Rio Grande do Sul (TJMRS**)**, considerando a infraestrutura híbrida (nuvem + local), a criticidade dos dados judiciais e a necessidade de conformidade com normas como MoReq-Jus e LGPD, o modelo Kaspersky Next EDR Optimum são os mais indicados. Este modelo oferece proteção especializada para servidores físicos e virtuais, além de gestão unificada de ambientes multicloud. Abaixo, detalhamos os modelos de prestação do serviço aplicáveis:

1.4.5.1 Diferentes modelos de prestação do serviço:

Para as licenças de antivírus Kaspersky Next EDR Optimum com gerenciamento, a ata da AL/MT prevê os seguintes modelos de prestação, aquisição e métricas:

· Licenciamento por Dispositivo: Cobrança baseada no número de endpoints (para EDR Optimum) e servidores (para Hybrid Cloud Security). Por exemplo, 300 endpoints + 50 servidores = 350 licenças.

· Gestão Híbrida: Suporte a implantações em nuvem (via Kaspersky Security Center Cloud Console) e on-premise (via console local), permitindo flexibilidade operacional para o TJMRS.

· Integração com SIEM: Exportação de logs de segurança via protocolos como Syslog para ferramentas de terceiros (ex.: Splunk, IBM QRadar), essential para auditoria e conformidade com MoReq-Jus.

1.4.5.2 Aquisição como Bem ou Serviço:

· Aquisição como Bem: As licenças são adquiridas como bens permanentes (software), com custo amortizado ao longo de 36 meses. Isso inclui direitos de uso, atualizações de threat intelligence e suporte técnico.

· Serviços Inclusos: A licença inclui serviços essenciais como suporte técnico 24/7, atualizações de assinaturas de ameaças e treinamento para a equipe do TJMRS. Não há opção de aquisição como serviço (SaaS) na ata, mas a gestão híbrida permite uso parcial de recursos em nuvem.

1.4.5.3 Ampliação ou Substituição da Solução:

· Ampliação: A aquisição de licenças adicionais é permitida via termo aditivo à ata, mantendo os preços originais do pregão. Por exemplo, se o TJMRS expandir sua frota de servidores, pode adquirir mais licenças sem novo processo licitatório.

· Substituição: A migração de soluções existentes (ex.: Kaspersky Select) para o EDR Optimum é suportada via ferramentas de importação do Kaspersky Security Center. Substituir por soluções de outros fabricantes exigiria novo pregão.

1.4.5.4 Métricas de Prestação e Pagamento:

A contratação será realizada pelo período de 36 (trinta e seis) contados a partir da emissão da ordem de fornecimento, podendo ser prorrogado sucessivamente, conforme os limites legais estabelecidos nos artigos 106 e 107 da Lei nº 14.133/2021, com pagamento conforme especificado no Termo de Referência e demais condições do edital.

Ø Métricas de Prestação:

§ Disponibilidade do Console: 99,9% de uptime para o Kaspersky Security Center.

§ Tempo de Resposta a Incidentes: Máximo de 4 horas para incidentes críticos.

§ Frequência de Atualizações: Atualizações de assinaturas de ameaças a cada 2 horas.

Ø Métricas de Pagamento:

§ Pagamento anual parcelado (3 parcelas anuais para cobrir os 36 meses), baseado no número de licenças ativas.

§ Penalidades por Descumprimento: Redução proporcional do valor em caso de indisponibilidade superior a 0,1% ou descumprimento de SLAs.

1.4.5.5 Ampliação ou substituição da solução implantada:

No caso do TJMRS, está sem proteção cibernética desde o segundo semestre do ano de 2023. Assim, a proposta é pela aquisição integral da solução, mediante contratação de empresa para aquisição de licença da solução de antivírus Kaspersky Next EDR Optimum com gerenciamento, para restabelecer a proteção cibernética das estações de trabalho, servidores e demais dispositivos de rede do Tribunal de

Justiça Militar do Estado do Rio Grande do Sul (TJM/RS), o que garantirá confiabilidade, eficiência e continuidade operacional.

1.4.6. Capacidade e alternativas do mercado de TIC

O mercado de Tecnologia da Informação e Comunicação (TIC) possui ampla capacidade para atender à demanda porlicença da solução de antivírus Kaspersky Next EDR Optimum com gerenciamento, oferecendo soluções consolidadas e tecnologicamente atualizadas. Diversas empresas especializadas atuam no fornecimento proposta, com contratos aderentes às exigências da Administração Pública.

Até o momento, não foram identificadas soluções livres ou públicas com maturidade suficiente para atender às exigências operacionais, de segurança da informação e rastreabilidade impostas pelo ambiente institucional do TJMRS.

1.4.7. Contratações correlatas e/ou interdependentes

Após análise da infraestrutura tecnológica atualmente disponível no Tribunal de Justiça Militar do RS, não foram identificadas contratações diretamente interdependentes que inviabilizem ou condicionem a presente aquisição de licenças da solução de antivírus Kaspersky Next EDR Optimum com gerenciamento.

Contudo, ressalta-se que o objeto apresenta correlação técnica e operacional com outras soluções de TIC já em uso no órgão, especialmente aquelas relacionadas à gestão de redes, monitoramento de ativos e políticas de segurança da informação. Tais interações são de caráter complementar, e não configuram dependência contratual obrigatória, mas devem ser consideradas na etapa de planejamento da implantação, a fim de assegurar a integração sistêmica **e a** continuidade dos serviços.

Adicionalmente, verifica-se que a presente contratação se alinha às políticas institucionais de governança digital e de segurança cibernética, em consonância com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e com as diretrizes estabelecidas no Plano Diretor de TIC (PDTIC) vigente neste Tribunal.

Portanto, conclui-se que não há contratações interdependentes que impeçam a execução do objeto, mas sim contratações correlatas que, em conjunto, reforçam a robustez da infraestrutura tecnológica e contribuem para a padronização e eficiência operacional no âmbito deste Tribunal.

A tabela a seguir apresenta o mapeamento dessas contratações correlatas:

Solução / Serviço	Objeto da Contratação	Relação com a Contratação do Antivírus	Natureza da Correlação
Infraestrutura de Rede (Switches e Wi-Fi Corporativo)	Aquisição de equipamentos de conectividade (Cisco Catalyst e APs Wi-Fi 6)	O antivírus atuará na proteção dos dispositivos que utilizam a rede corporativa.	Complementar
Firewall e Segurança Perimetral	Solução de firewall de próxima geração (NGFW)	Integração necessária para ampliar a defesa em camadas, evitando sobreposição de regras.	Complementar
Gestão de Identidade e Acessos (AD/LDAP)	Serviços de autenticação e controle de usuários	O antivírus se integra aos diretórios de autenticação para aplicação de políticas de segurança.	Complementar
Backup e Armazenamento em Nuvem	Soluções de backup corporativo	O antivírus garante a integridade dos arquivos armazenados e evita propagação de malware.	Complementar
Plataforma de Monitoramento e Controle (SIEM/SOC)	Serviços de monitoramento de eventos de segurança	O antivírus fornece logs e alertas que serão consumidos pelo SOC para correlação de eventos.	Complementar

1.5. Análise dos Custos Totais da Demanda

A análise comparativa de preços, realizada a partir da pesquisa de mercado e do Mapa Comparativo de Preços, permitiu identificar o valor médio de R$ 794,50 por endpoint/ano para a solução antivírus Kaspersky Next EDR Optimum com gerenciamento. Esse valor reflete a média ponderada das propostas levantadas, conferindo maior precisão e transparência à estimativa.

Memória de Cálculo

Solução Avaliada: Kaspersky Next EDR Optimum

Preço Unitário Referencial: R$ 794,50 / endpoint / ano

Quantidade de Endpoints: 250

Período de Contratação: 36 meses (com possibilidade de prorrogação, nos termos da Lei nº 14.133/2021, art. 107).

Cálculo do Investimento Total Estimado:

Valor Total=Preço Unitário×Quantidade de Endpoints×Período (anos)Valor\ Total = Preço\ Unitário \times Quantidade\ de\ Endpoints \times Período\ (anos)Valor Total=Preço Unitário×Quantidade de Endpoints×Período (anos)
Exemplo (com 250 endpoints):

794,50×250×1=R$ 198.625,00
Aspectos Técnicos e Econômicos

Custo Total de Propriedade (TCO):

Inclui o custo de aquisição das licenças, suporte técnico, instalação, gerenciamento, atualizações de software, e eventuais treinamentos. Considerando a contratação por meio de Ata de Registro de Preços, assegura-se maior economicidade e simplificação administrativa.

Benefícios Qualitativos:

· Proteção avançada contra ameaças cibernéticas, com recursos de EDR (Endpoint Detection and Response).

· Conformidade com a LGPD e com as boas práticas de governança de TIC no setor público.

· Gestão centralizada e em nuvem, reduzindo custos operacionais com infraestrutura própria.

· Integração com SIEMs existentes, favorecendo a interoperabilidade com os sistemas do órgão.

Justificativa da Escolha:

Apesar de alternativas como Microsoft Defender (R$ 495,72) e Trend Micro Vision One (R$ 325,00) apresentarem custo inferior no curto prazo, a solução Kaspersky Next EDR Optimum foi considerada a mais vantajosa para o TJM/RS, por aliar robustez técnica, maior nível de conformidade com MoReq-Jus, e maturidade no mercado, reduzindo riscos operacionais.

Quantidade de Endpoints	Preço Unitário (R$/endpoint/ano)	Prazo (anos)	Investimento Total Estimado (R$)	Observações Técnicas
100	794,50	3	79.450,00	Licenciamento anual, gestão em nuvem, suporte incluso.
200	794,50	3	158.900,00	Escalabilidade da solução sem perda de desempenho.
250	794,50	3	198.625, 00	Custo justificado pela robustez técnica e conformidade com MoReq-Jus e LGPD.

Considerações Técnicas

1. Memória de Cálculo:

   Valor Total=Preço Unitário×Nº Endpoints×PrazoValor+Gerenciamento Total = Preço\ Unitário \times Nº\ Endpoints \times Prazo\gerenciamentoValor Total=Preço Unitário×Nº Endpoints×Prazo+gerenciamento

   Exemplo para 250 endpoints+ 01 gerenciamento:

794,50×250×1=R$198.625, 00794,50 \times 250 \times 1= R$ 198.625, 00 794,50×250×1=R$198.625, 00

Custos Relevantes Incluídos no TCO:

   a. Licenciamento anual (inclui atualizações contínuas).

   b. Suporte técnico especializado.

   c. Acesso a console de gerenciamento em nuvem.

   d. Recursos de EDR (Endpoint Detection and Response) com integração a SIEM.

2. Aspectos de Economicidade:

   a. Contratação por adesão a Ata de Registro de Preços, garantindo melhores condições comerciais.

b. Escalabilidade flexível, com pagamento proporcional ao número de endpoints contratados.

c. Redução de custos indiretos com infraestrutura própria, já que o gerenciamento é em nuvem.

Tabela Comparativa de TCO – 250 Endpoints (1 ano)

Solução	Preço Unitário (R$/endpoint/ano)	Nº Endpoints	Prazo (anos)	Investimento Total (R$)	Observações Técnicas
Kaspersky Next EDR Optimum	**794,50**	**250**	**1**	**198.625, 00**	**EDR completo, gestão em nuvem, integração SIEM, alta conformidade MoReq-Jus e LGPD.**
Microsoft Defender	495,72	250	1	123.930,00	Boa integração nativa com Windows/Azure. Conformidade moderada.
CrowdStrike Falcon	1.735,00	250	1	433.750,00	Solução de ponta com IA avançada, indicada para ambientes de altíssimo risco. Alto custo.
Trend Micro Vision One	325,00	250	1	81.250,00	Custo reduzido, proteção multi-camada. Funcionalidades limitadas frente a soluções mais robustas.

Análise Técnica e Econômica

1. Kaspersky Next EDR Optimum

· Melhor equilíbrio entre custo e robustez técnica.

· Inclui gestão centralizada em nuvem, mitigando custos de infraestrutura local.

· Alinhado às exigências de segurança corporativa, LGPD e MoReq-Jus.

· Custo total intermediário, viabilizando economicidade sem comprometer a segurança.

2. Microsoft Defender

· Mais barato em termos absolutos.

· Forte integração com ecossistema Microsoft (Windows e Azure).

· Porém, possui menor abrangência de funcionalidades EDR avançadas e dependência da plataforma Microsoft.

3. CrowdStrike Falcon

· Solução tecnicamente superior, com IA preditiva e resposta automatizada.

· Custo muito elevado (mais do que o dobro da solução Kaspersky), o que compromete a economicidade no contexto da Administração Pública.

4. Trend Micro Vision One

· Mais barato do grupo, mas com funcionalidades limitadas frente a ambientes corporativos complexos.

· Pode atender cenários básicos, mas não assegura a robustez exigida pelo TJM/RS em termos de conformidade e alta resiliência cibernética.

Justificativa da Escolha

Considerando o disposto no art. 14 da Lei nº 14.133/2021**, a vantajosidade econômica não se limita ao menor preço, mas à solução que melhor assegura o** equilíbrio entre custo, desempenho, segurança e ciclo de vida**.**

O Kaspersky incorporou recursos avançados de inteligência artificial, machine learning e criptografia de dados confidenciais, oferecendo

funcionalidades como Kaspersky Password Manager, código de cofres protegidos e monitoramento de comportamento suspeito em tempo real. Tais ferramentas são especialmente relevantes considerando o uso do sistema Eproc pelo TJMRS — sistema essencialmente web-based, acessado por diferentes perfis de usuários (juízes, servidores, advogados), e que exige segurança reforçada para dados sensíveis, logins e certificados digitais.

Destaca-se está versão que atende perfeitamente às exigências do ambiente institucional, destacando-se na proteção para redes, ambientes com servidores, dispositivos móveis e trabalho remoto, reforçando a adequação da solução ao perfil do órgão. Além da proteção convencional contra malwares e ameaças online, o Kaspersky se diferencia por ser uma verdadeira plataforma de proteção de endpoint (EPP – Endpoint Protection Platform), oferecendo um conjunto mais completo de funcionalidades, como análise comportamental, gerenciamento de vulnerabilidades, controle de dispositivos e segurança de rede em nível avançado.

Essa característica é especialmente importante no contexto do TJMRS, onde o EproC, sistema essencialmente web, é acessado por diversos perfis de usuários e exige alta confiabilidade na proteção de dados sensíveis, senhas e certificados digitais. O Kaspersky é o único entre os antivírus avaliados que oferece uma camada específica de proteção contra ameaças de rede em endpoints, com capacidade de detectar, bloquear e neutralizar ataques diretamente no tráfego de rede de entrada, antes que alcancem o dispositivo ou comprometam os dados inseridos no sistema.

Como endpoints são todos os dispositivos que se conectam a rede — como computadores, laptops, servidores e máquinas virtuais — e representam pontos críticos de vulnerabilidade, a proteção oferecida por uma plataforma de endpoint é essencial para a integridade e segurança das informações que circulam nos sistemas do Tribunal. Por isso, a escolha do antivírus Kaspersky Next EDR Optimum com gerenciamento, garante uma cobertura de segurança mais ampla e adequada às demandas institucionais do TJMRS, oferecendo uma camada superior de proteção que justifica a sua permanência como solução oficial de antivírus, mesmo em comparação com opções de menor custo nominal.

Embora o custo da solução Kaspersky possa ser superior ao de alternativas como o Avast, sua eficiência operacional, confiabilidade, proteção abrangente e aderência às necessidades específicas do TJMRS tornam sua aquisição mais vantajosa em termos econômicos globais.

A Contratação garantirá a continuidade da proteção cibernética já consolidada desde 2015 com o uso da solução Kaspersky, reconhecida por sua robustez, confiabilidade e aderência às necessidades institucionais do TJMRS. Tal escolha está em conformidade com os princípios da economicidade (art. 11, III) e da seleção da proposta mais vantajosa (art. 5º), bem como com o critério de julgamento por menor preço global (art. 33, I) da Lei nº 14.133/2021, considerando a eficiência e a melhor relação entre custos e benefícios (art. 6º, XL).

Em resumo, a lei busca um equilíbrio entre a busca pela menor despesa e a seleção da proposta que oferece as melhores condições para a administração pública, garantindo a eficiência (é o que executa uma tarefa com qualidade, competência, excelência, com nenhum ou com o mínimo de erros) no uso dos recursos públicos.

Portanto, a escolha pela solução antivírus Kaspersky Next EDR Optimum com gerenciamento atende ao interesse público, promove segurança institucional, reduz riscos operacionais e aperfeiçoa o uso de recursos humanos e tecnológicos, assegurando o cumprimento do princípio da eficiência e da economicidade na sua plenitude.

Assim, a escolha das 250 licenças Kaspersky Next EDR Kaspersky Next EDR Optimum com gerenciamento é a mais apropriada, pois:

· Garante alto nível de segurança cibernética compatível com o ambiente do TJM/RS.

· Possui **c**usto intermediário, que se mostra sustentável no ciclo de vida contratual.

· Está aderente às normativas nacionais e internacionais de segurança da informação, assegurando conformidade e governança.

· Permite escalabilidade, acompanhando o crescimento da rede sem comprometer o orçamento.

Componente de Custo	Valor (R$)	Periodicidade
Custo mensal total (250licenças)	5.517,36	Mensal

Componente de Custo	Valor (R$)	Periodicidade
Custo anual total (250licenças)	198.625, 00	36 meses

Memória de cálculo:

· **Custo fixo 36 meses**:

Média do Banco de Preços: R$ 794,50/licenças × 250 licenças = **R$ 198.625, 00 total**

(Fonte: Banco de Preços, com média validada (R$ 794,50) e desvio padrão de 47,76%).

· **Vantagens incorporadas**:

Atualização tecnológica contínua (sem custos adicionais).

Transferência de riscos operacionais (falhas).

Redução de custos ocultos (gestão, indisponibilidade).

b) Memória de cálculo e origem dos dados

Os valores referentes à aquisição de licença da solução de antivírus Kaspersky Next EDR Optimum com gerenciamento foram extraídos do relatório de preços públicos no sistema https://www.bancodeprecos.com.br/, considerando os itens classificados sob os códigos CATMAT/CATSER específicos.

Foi utilizada a média aritmética de R$ 794,50 por licença, com base em valores validados e excluídos os excessivamente elevados, conforme relatório com desvio padrão de 47,76%.

Conclusão técnica

Embora a projeção de custo direto anual para a contratação das 250 licenças da solução Kaspersky Next EDR Optimum com gerenciamento (R$ **198.625, 00**) possa parecer, em um primeiro momento, um investimento relevante, a análise sob a ótica do custo total de propriedade (TCO – Total Cost of Ownership) demonstra que a opção é a mais vantajosa e sustentável para o TJM/RS.

Modelos alternativos, baseados em soluções menos robustas ou com menor custo unitário, apresentam fragilidades significativas, pois transferem ao órgão contratante parte da responsabilidade operacional e dos riscos associados à manutenção da segurança cibernética, como a necessidade de suporte técnico adicional, riscos de falhas de integração, obsolescência precoce ou conformidade insuficiente com normativos como a LGPD e o MoReq-Jus. Esses fatores acarretam custos ocultos não mensurados no momento da aquisição inicial, mas que impactam diretamente a continuidade dos serviços jurisdicionais e a governança da informação.

Por outro lado, a solução Kaspersky Next EDR Optimum com gerenciamento transfere à contratada não apenas a licença de uso, mas também o gerenciamento centralizado em nuvem, a integração com SIEM, a gestão de patches e a suporte avançado de EDR (Endpoint Detection and Response). Isso mitiga riscos de falhas operacionais e assegura padronização, rastreabilidade e estabilidade operacional, sem a necessidade de estruturas adicionais internas para manter a solução em pleno funcionamento.

Adicionalmente, o contrato prevê atualizações automáticas e contínuas da solução, garantindo que os endpoints estejam sempre protegidos contra novas ameaças cibernéticas e mitigando riscos de obsolescência tecnológica precoce. Esse modelo evita futuros aportes orçamentários imprevistos com substituições emergenciais de solução ou reforços de segurança decorrentes de incidentes não prevenidos.

Sob a ótica econômica, o custo total da solução Kaspersky, embora não seja o menor no mercado, torna-se mais eficiente no médio e longo prazo, quando comparado aos riscos de indisponibilidade, falhas de proteção ou necessidade de substituição prematura em modelos alternativos. Além disso, sua conformidade plena com requisitos legais e normativos reforça sua adequação institucional.

Assim, considerando os princípios previstos no art. 14 da Lei nº 14.133/2021, especialmente os da eficiência, economicidade, planejamento, transparência e interesse público, conclui-se que a escolha do Kaspersky Next EDR Optimum com gerenciamento representa a alternativa mais vantajosa para a Administração, assegurando eficácia operacional, proteção da informação e otimização do uso dos recursos públicos.

	Nr.	Soluções identificadas	Especificação do produto/serviço*	Catmat/Catser	Quantificação do Produto ou Serviço*	Órgão (s) que adotaram a solução	Vantagens e Benefícios*	Desvantagens e riscos	Custo(s) envolvido(s) anual
1	Microsoft Defender for Endpoint		Solução EDR integrada ao ecossistema Microsoft, oferecendo proteção avançada, investigação de incidentes e resposta automatizada. Inclui proteção em tempo real, análise de comportamento e integração com o Azure Sentinel.	26077	250	-	Integração nativa com Windows e Office 365, ideal para ambientes Microsoft.	Pode requerer configuração adicional para ambientes heterogêneos (Linux/macOS).	R$ 123.930,00
2	CrowdStrike Falcon Insight		Plataforma EDR baseada em nuvem, com detecção de ameaças em tempo real, caça proativa a ameaças e resposta automatizada. Utiliza IA para análise comportamental.	350949	250		Alta escalabilidade e baixo impacto no desempenho dos endpoints.	Custos mais elevados em comparação com soluções básicas.	R$ 433.750,00
3	Kaspersky Next EDR Optimum		Solução EDR autônoma com proteção preventiva, detecção de ameaças e resposta automatizada. Inclui recursos de IA e análise de comportamento, projetada para segurança abrangente e econômica.	350949	250	AL/MT	Oferece segurança avançada com recursos como detecção, resposta a ameaças e automação.	Pode exigir mais conhecimento técnico para configuração e gerenciamento.	R$ **198.625,00**

	Nr.	Soluções identificadas	Especificação do produto/serviço*	Catmat/Catser	Quantificação do Produto ou Serviço*	Órgão (s) que adotaram a solução	Vantagens e Benefícios*	Desvantagens e riscos	Custo(s) envolvido(s) anual
4	Trend Micro Vision One		Plataforma XDR (Extended Detection and Response) que combina EDR com proteção de e-mail, rede e nuvem. Oferece visibilidade unificada e resposta integrada.	350949	250		Escopo ampliado (XDR) com integração multicamada.	Complexidade inicial na implementação.	R$ 81.250,00

*Observações:

• Especificação do produto/serviço: indicar os serviços e materiais a serem utilizados, explicitando ainda fornecedores e fabricantes potencialmente aptos ao atendimento dos requisitos especificados.

• Quantificação do Produto ou Serviço: Apresentar ou mencionar anexo como foi quantificada a estimativa das opções levantadas

• Vantagens e Benefícios: Descrever benefícios diretos e indiretos em termos de economicidade, eficácia, eficiência, e de melhor aproveitamento dos recursos.

1.6. Escolha e Justificativa da Solução

1.6.1. Descrição da Solução Escolhida

A solução selecionada consiste na aquisição de 250 licenças da solução Kaspersky Next EDR Optimum com gerenciamento, para restabelecer a proteção cibernética das estações de trabalho, servidores e demais dispositivos de rede do Tribunal de Justiça Militar do Estado do Rio Grande do Sul (TJM/RS). Atualmente expostos a vulnerabilidades devido à ausência de um software antivírus ativa, a solução atenderá às necessidades das unidades do Tribunal, incluindo a 1ª, 2ª Auditorias Militares, Santa Maria e Passo Fundo, garantindo a continuidade dos serviços jurisdicionais e administrativos com segurança e eficiência.

O modelo de aquisição é Adesão a Ata de Registro de Preços, com contratação de licenças por um período de 36 (trinta e seis) meses, prorrogável conforme artigo 107 da Lei nº 14.133/2021. O modelo é aderente aos princípios da economicidade, eficiência e previsibilidade orçamentária permitindo a previsibilidade orçamentária e a obtenção de um custo total de propriedade (TCO) mensurável,

Motivação e Justificativa da Escolha: A escolha pela aquisição por Adesão a Ata de Registro de Preços das licenças para um período fixo decorre de uma análise criteriosa de custo total de propriedade (TCO), que, neste caso, se concentra no valor de aquisição e gerenciamento sem custos adicionais. A solução Kaspersky Next EDR Optimum, combinada com o gerenciamento via servidor on-premise, proporciona uma resposta eficaz e previsível para a necessidade de proteção. A aquisição de licenças por um período fixo elimina riscos de custos indiretos com manutenção e obsolescência.

Este modelo de contratação transfere para a solução a responsabilidade técnica e logística de proteção dos ativos, ao mesmo tempo em que permite à Administração manter o controle estratégico sobre sua infraestrutura. A escolha da solução via Ata de Registro de Preços proporciona um processo ágil e aderente aos princípios da economicidade, eficiência e previsibilidade.

1.6.2 Benefícios Esperados

A adoção da solução de segurança proporcionará uma série de benefícios operacionais e estratégicos ao TJM/RS, tais como:

1 . Aumento da eficácia na execução de atividades administrativas e jurisdicionais por meio da proteção proativa contra ameaças cibernéticas e da garantia de continuidade operacional.

2. Maior eficiência na alocação de recursos públicos e na força de trabalho da área de TI, que poderá focar em atividades estratégicas, em vez de atuar na gestão de incidentes.

3. Padronização tecnológica do parque de endpoints e servidores, com ganhos em interoperabilidade, rastreabilidade e conformidade com as políticas de segurança da informação.

4. Agilidade e segurança nos processos internos por meio da detecção e resposta automatizada a ameaças.

5. Redução de vulnerabilidades e riscos associados à ausência de uma solução de segurança de ponta.

1.6.3 Resultados Esperados

Com a implantação da solução contratada, espera-se alcançar resultados objetivos em termos de economicidade, controle operacional e desempenho institucional. Os principais resultados esperados incluem:

· Aumento da segurança da informação e da resiliência do ambiente tecnológico do Tribunal.

· Redução da necessidade de ações reativas de resposta a incidentes de segurança.

· Disponibilização de equipamentos sempre protegidos e operacionais.

· Melhor aproveitamento da força de trabalho interna, com foco em atividades estratégicas e de apoio à gestão.

· Atendimento integral às diretrizes de planejamento, economicidade e racionalidade administrativa, estabelecidas pela Lei nº 14.133/2021 e pelas orientações de órgãos de controle.

- Atendimento integral às diretrizes de planejamento, economicidade e racionalidade administrativa, estabelecidas pela Lei nº 14.133/2021 e pelas orientações de órgãos de controle.

Demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis, Lei Federal nº 14.133/2021, Art. 18, § 1º, inciso IX.

1.6.4. Relação entre a Demanda Prevista e a quantidade de bens e/ou serviços Contratados

1**.** Unidade de Medida e Quantitativo de Equipamentos

· Unidade de medida do serviço: Licença (incluindo hardware, suporte, manutenção, insumos e software).

· Quantidade de licenças: 250 licenças de Kaspersky Next EDR Optimum com gerenciamento.

Justificativa:

· Baseado no diagnóstico operacional do Tribunal, 250 licenças de EDR cobrem a totalidade os ativos a serem protegidos nas unidades do Tribunal.

1. Composição do Custo Mensal por Equipamento

O custo total da contratação para os 36 meses foi calculado com base no valor unitário das licenças de EDR e no valor fixo de gerenciamento.

Custo das Licenças: 250 licenças × R$ 794,50 = R$ 198.625,00

Valor Total da Contratação:

R $198.625,00 (licenças)=R$ R$ 198.625,00

2. Cálculo do Custo Total para 250 licenças de EDR

A análise do custo total da contratação é baseada em uma estrutura transparente e objetiva, que reflete os valores da solução de segurança para o período de 36 meses. O cálculo detalhado a seguir considera a quantidade de licenças necessárias para cobrir os equipamentos do Tribunal de Justiça Militar do Estado do Rio Grande do Sul (TJM/RS).

A estrutura de custo para a solução de segurança cibernética é composta por dois componentes principais: o custo das licenças de proteção para cada equipamento (endpoint) incluído o gerenciamento da solução.

3.1. Custo das Licenças Kaspersky Next EDR Optimum:

Este valor representa o custo individual para a proteção de cada uma das 250 estações de trabalho e dispositivos de rede. O preço unitário já abrange o período total de 36 meses.

· Valor unitário para 36 meses: R$ 794,50

· Quantidade: 250 equipamentos

· Cálculo: 250 equipamentos × R$ 794,50 = R$ 198.625,00

Tabela de Composição do Custo Total da Contratação

Descrição do Item	Unidade de Medida	Quantidade	Preço Unitário (36 meses)	Valor Total
Kaspersky Next EDR Optimum	Licença	250	R$ 794,50	R$ 198.625,00
Custo Total da Contratação (36 meses)				**R$ 198.625,00**

3.2**.** Origem e Validação dos Parâmetros

Parâmetro	Fonte	Validação Científica
Custo fixo por equipamento	Banco de Preços do Governo (CATMAT/CATSER)	- Média: R$ 794,50 (mediana: R$ 794,50); - Desvio padrão: 47,76% (superior ao aceitável para serviços públicos); - Outliers excluídos (ex.: R$ 1.240,50 e 358,14).

1.6.5. Estimativa do Custo Total da Solução Escolhida

A memória de cálculo demonstra que o custo estimado de R$ R$ 198.625,00 para 250 (duzentas e cinquenta) licenças Kaspersky Next Edr Optimum com gerenciamento, é tecnicamente robusto, com parâmetros validados por fontes oficiais e alinhados à demanda real do tribunal. A unidade de medida (custo/software) assegura transparência, escalabilidade e conformidade com a Lei 14.133/2021, viabilizando uma contratação pública eficiente e livre de distorções. Recomenda-se sua adoção para garantia de continuidade operacional e melhor utilização de recursos.

As estimativas de custo para a aquisição das licenças de antivírus foi definida com base em pesquisa realizada nos principais sites eletrônicos oficiais de contratações públicas e complementada por cotações obtidas junto a fornecedores especializados no mercado. O preço estimado para a contratação, é de R$ **794,50 (setecentos e noventa e quatro reais com cinquenta centavos)** unitário e o valor de **R$ 198.625,00 (cento e noventa e oito mil seiscentos e vinte reais)**, contempla a aquisição de **250 licenças com gerenciamento** pelo período de 36 meses, **up front 3 anos**.

A Dotação Orçamentária a ser utilizada nesta contratação:Recurso: 2002, Unidade Orçamentária: 07.01, Atividade/Projeto: 3902, Natureza da Despesa: 3.3.90.40 - Serv. Tic - Pess. Jurídica.

Obs.: Poderão constar de anexo classificado, se a Administração optar por preservar o seu sigilo até a conclusão da licitação (Lei Federal n.º 14.133/2021, art. 18, §1, inciso VI).

1.7. Declaração de viabilidade da contratação

1.7. Declaração de viabilidade da contratação

A Equipe de Planejamento da Contratação, com fundamento nos estudos técnicos e análises de custo realizadas, DECLARA VIÁVEL a contratação de 250 (duzentas e cinquenta) licenças Kaspersky Next Edr Optimum com gerenciamento para o Tribunal de Justiça Militar do Rio Grande do Sul, nos termos abaixo justificados:

· Atendimento à demanda

· Eficiência de custos

· Conformidade com a Lei 14.133/2021

CAPÍTULO 2: SUSTENTAÇÃO DO CONTRATO

2.1. Adequação do Ambiente

Para a execução contratual da aquisição de licenças Kaspersky Next Edr Optimum com gerenciamento, o ambiente do TJMRS encontra-se tecnicamente compatível com os requisitos operacionais exigidos. Em relação à infraestrutura tecnológica, todas as unidades já dispõem de rede elétrica e lógica suficientes para a instalação dos equipamentos. A infraestrutura elétrica existente comporta a demanda de energia dos dispositivos, sem necessidade de adaptações adicionais.

Quanto à logística de implantação, ocorrerá conforme cronograma acordado com a contratada, em pontos previamente definidos. O espaço físico e os mobiliários existentes nas unidades são adequados para o recebimento dos dispositivos, sem a necessidade de intervenções estruturais.

O impacto ambiental do serviço é reduzido, pois não há geração significativa de resíduos e o fornecimento de equipamentos modernos trará ganho de eficiência energética, alinhando-se aos princípios de sustentabilidade da administração pública.

2.2. Recursos Materiais e Humanos

Não há necessidade de outras contratações para viabilizar a execução do contrato. Quanto aos recursos humanos, os servidores atualmente lotados na área administrativa estão capacitados para operara a solução. Caso necessário, a contratada poderá oferecer treinamento pontual sobre a instalação e o uso licenças Kaspersky Next Edr Optimum com gerenciamento.

2.3. Continuidade do Fornecimento

A eventual descontinuidade do contrato poderia comprometer atividades administrativas essenciais. Por isso, o contrato incluirá cláusulas de transição para manutenção mínima da prestação do serviço em casos de rescisão ou falhas operacionais. Entre as hipóteses de interrupção estão o inadimplemento contratual, falência da empresa ou descumprimento de cláusulas técnicas. Nesses casos, o TJMRS poderá recorrer a soluções alternativas emergenciais, incluindo contratação direta por tempo determinado da solução de licenças Kaspersky Next Edr Optimum com gerenciamento.

2.4. Transição Contratual e encerramento do contrato

1. Transição Contratual

A fase de transição ocorre na proximidade do término do contrato de 36 meses ou em caso de não prorrogação. As ações a seguir são cruciais para um processo sem interrupções:

· Planejamento Antecipado: Iniciar o planejamento da transição com antecedência mínima de 90 dias antes do término do contrato. Isso inclui a definição de um cronograma, a alocação de equipe técnica e a identificação de uma nova solução de segurança, caso a prorrogação não seja viável.

· Renegociação ou Nova Licitação: Avaliar a prorrogação do contrato atual, conforme previsto na Lei nº 14.133/2021, ou iniciar um novo processo licitatório para a contratação de uma nova solução.

· Migração de Dados e Configurações: Se uma nova solução for escolhida, a equipe de TI deve planejar a migração de configurações e dados de segurança. Isso inclui a exportação de políticas de proteção, listas de exclusão, logs de eventos e outras configurações importantes do Kaspersky Security Center para a nova plataforma.

· Implantação da Nova Solução: A nova solução deve ser instalada em ambiente de teste para validação técnica antes de sua implantação em produção. A implantação deve ser faseada para minimizar riscos, garantindo que os novos agentes de segurança estejam totalmente

operacionais antes da desinstalação dos agentes da Kaspersky.

1. Encerramento do Contrato

O encerramento do contrato é o procedimento final, que formaliza o término da relação jurídica. Os seguintes passos são essenciais:

· Desinstalação do Software: Após a garantia de que a nova solução está funcionando plenamente em todos os dispositivos, proceder à desinstalação remota dos agentes da Kaspersky (EDR Optimum) e, por fim, do console de gerenciamento Kaspersky Security Center.

· Auditoria Final e Relatório de Encerramento: A equipe técnica deve realizar uma auditoria para confirmar que todos os softwares da Kaspersky foram removidos e que o ambiente de TI está seguro. Um relatório de encerramento deve ser elaborado, documentando o processo de transição, as ações realizadas e o estado final do parque tecnológico.

· Formalização do Encerramento: Emitir um termo de encerramento do contrato, atestando o cumprimento de todas as obrigações por ambas às partes e formalizando o fim da vigência. Isso inclui a confirmação de que os dados de segurança e as informações do TJM/RS foram tratados de forma segura e que não há pendências financeiras ou técnicas.

2.5. Estratégia de Independência Tecnológica

2.5. Estratégia de Independência Tecnológica

A estratégia de independência tecnológica visa garantir que o Tribunal de Justiça Militar do Rio Grande do Sul (TJM/RS) não se torne excessivamente dependente de um único fornecedor, tecnologia ou modelo de serviço, minimizando os riscos de `lock-in` tecnológico. Para a contratação da solução de segurança cibernética, essa abordagem se manifesta em ações de planejamento e gestão, assegurando a flexibilidade e a autonomia do órgão no longo prazo.

1. Plano de Migração e Transição

O primeiro pilar da independência tecnológica é um plano de migração e transição bem definido. Este plano deve ser elaborado antes mesmo da assinatura do contrato e visa garantir uma saída ordenada e segura, caso haja a necessidade de substituir a solução ou o fornecedor ao término da vigência contratual. Elementos-chave incluem:

· Padrões Abertos: Priorizar soluções que utilizem padrões de mercado abertos para interoperabilidade.

· Capacidade Técnica Interna: Capacitar à equipe de TI do Tribunal para gerenciar a solução, reduzindo a dependência de suporte externo para operações rotineiras.

· Portabilidade de Dados: Assegurar que os dados e configurações de segurança (como políticas, logs e configurações de firewall) possam ser facilmente exportados para formatos compatíveis com outras plataformas.

2. Governança e Gestão de Riscos

Uma governança robusta é essencial para evitar o `lock-in`. A estratégia de independência tecnológica exige:

· Avaliação Contínua de Mercado: Acompanhar as inovações e as alternativas de mercado em soluções de segurança para identificar possíveis substitutos ou tecnologias mais avançadas.

· Análise de Custo-Benefício: A cada ciclo de contratação, realizar uma nova análise de custo-benefício e do TCO (Custo Total de Propriedade) para comparar a solução atual com as disponíveis no mercado.

· Cláusulas Contratuais: Incluir no contrato cláusulas que garantam a desmobilização assistida e a transferência de conhecimento por parte da contratada, caso o contrato não seja renovado.

3. Diversificação de Tecnologia

Para evitar a dependência, o TJM/RS pode considerar a diversificação de tecnologias em diferentes camadas da segurança cibernética. Embora a contratação de um único fornecedor para EDR seja eficiente, a estratégia de longo prazo pode envolver a busca por soluções de `SIEM`, `SOAR` ou `DLP` de outros fornecedores, permitindo a criação de um ecossistema de segurança mais resiliente e adaptável.

CAPÍTULO 3: ESTRATÉGIA PARA A CONTRATAÇÃO

3.1. Natureza do Objeto

A presente contratação consiste na aquisição de licenças de software de segurança cibernética da Kaspersky, incluindo a solução Kaspersky Next EDR Optimum e o gerenciamento via Kaspersky Security Center. O objetivo é restabelecer a proteção dos ativos de TI do Tribunal de Justiça Militar do Estado do Rio Grande do Sul (TJM/RS), que se encontram vulneráveis.

A natureza da despesa enquadra-se como despesa corrente, uma vez que a contratação de software como serviço (SaaS) ou o licenciamento por período determinado é um serviço continuado, conforme o art. 6º, inciso XXIII, da Lei nº 14.133/2021. Trata-se de um serviço essencial e de natureza estratégica para a rotina institucional, pois a proteção de dados e a segurança da infraestrutura de TI são atividades permanentes e cruciais para a continuidade dos serviços jurisdicionais e administrativos do Tribunal.

Quanto à propriedade intelectual, a presente contratação não envolve o desenvolvimento de software personalizado nem a produção de ativos tecnológicos exclusivos. As licenças adquiridas são de propriedade da fornecedora, e o Tribunal adquire apenas o direito de uso temporário durante a vigência do contrato. Todos os dados gerados pelo uso da solução (ex.: logs de eventos, relatórios de ameaças) são de propriedade do TJM/RS e deverão ser entregues em formato aberto e reutilizável ao final da contratação.

Portanto, o objeto possui natureza de serviço continuado de despesa corrente, com uso temporário de software e sem desenvolvimento de propriedade intelectual exclusiva por parte da contratada.

3.2. Parcelamento do Objeto e Adjudicação

O objeto da presente contratação—a aquisição de licenças de segurança cibernética para proteção de endpoints e gerenciamento centralizado—não será parcelado, pois a solução é considerada indivisível. A unificação do contrato em um único fornecedor e lote são essenciais para a compatibilidade tecnológica, a integração da solução e a eficiência na gestão. O fracionamento entre diferentes fornecedores implicaria em riscos técnicos e operacionais, como a falta de interoperabilidade entre as licenças e o console de gerenciamento, a duplicidade de suporte e o aumento de custos, contrariando os princípios da eficiência e da economicidade previstos nos §§ 2º e 3º do art. 40 e § 1º do art. 47 da Lei nº 14.133/2021.

3.2.1. Adjudicação do Objeto

A adjudicação do objeto será realizada em lote único, tendo em vista que se trata de uma solução integrada, onde as licenças de proteção e a capacidade de gerenciamento se inter-relacionam de forma indivisível. A contratação unificada assegura a homogeneidade tecnológica, a facilidade de gestão contratual e a eficiência operacional, sendo incompatível com a fragmentação por itens ou componentes.

Adicionalmente, o fracionamento acarretaria potenciais conflitos operacionais, como a falta de comunicação entre os agentes de segurança e a plataforma de gerenciamento, dificuldades na fiscalização e no controle de desempenho. Esses riscos comprometem o atendimento ao interesse público, razão pela qual a adjudicação por lote único se revela a forma mais vantajosa para a Administração, conforme disposto nos arts. 15 e 122 da Lei nº 14.133/2021. Não será permitida a participação em consórcio, considerando a viabilidade de execução do objeto por empresas individualmente habilitadas.

3.2.2. Subcontratação do Objeto

A subcontratação parcial será admitida, desde que previamente autorizada pela Administração e restrita a atividades acessórias. No caso da aquisição de licenças de software, entende-se por serviços acessórios aqueles relacionados ao suporte técnico de primeiro nível, treinamento básico de usuários ou apoio na implantação inicial. A empresa contratada continuará responsável integral pela execução do contrato e pelos serviços subcontratados, conforme o art. 122 da Lei nº 14.133/2021. A vedação à subcontratação da atividade-fim (o fornecimento e a manutenção da funcionalidade das licenças) assegura que a Administração mantenha uma relação direta com o fornecedor principal, garantindo a integridade e a segurança do serviço contratado.

3.3. Modalidade e Tipo de Licitação

A modalidade de contratação selecionada é a **Adesão à Ata de Registro de Preços**. O Tribunal de Justiça Militar do Rio Grande do Sul (TJM/RS) irá aderir à Ata de Registro de Preços já homologada pela Assembleia Legislativa do Estado do Mato Grosso (AL/MT), para a aquisição das licenças Kaspersky Next EDR Optimum.

Essa modalidade dispensa a necessidade de um novo processo licitatório, pois o Tribunal adere aos termos e condições já definidos e homologados em um certame anterior. Assim, o critério de julgamento de menor preço global já foi estabelecido e observado na licitação original, garantindo que a contratação seja a mais vantajosa para a Administração Pública, conforme o princípio da economicidade.

3.4 Vigência do contrato

A vigência do contrato será de 36 (trinta e seis) meses**,** prazo este que atende aos critérios estabelecidos no art. 107 da Lei nº 14.133/2021**,** que permite a prorrogação dos contratos de serviços contínuos por até 10 anos, desde que haja vantagem para a Administração.

Esse período foi definido com base nos seguintes fundamentos, que refletem a natureza estratégica e a complexidade de uma solução de segurança cibernética:

ü Ganhos em Economicidade e Otimização de Custos: Contratos de longa duração, como o de 36 meses, permitem que a Administração obtenha preços mais competitivos junto ao mercado. Os fornecedores de software de segurança frequentemente oferecem valores unitários mais baixos para compromissos de múltiplos anos, o que se traduz em uma economia substancial para o Tribunal quando comparado a contratos anuais sucessivos. Essa previsibilidade financeira permite um melhor planejamento orçamentário.
ü Amadurecimento da Postura de Segurança: A plena eficácia de uma solução de segurança como o Kaspersky Next EDR Optimum não é alcançada imediatamente após a sua implantação. São necessários meses para que a equipe técnica do Tribunal configure, ajuste e otimize as políticas de segurança, integre o sistema com outras ferramentas existentes e aprimore a capacidade de detecção e resposta a incidentes. Um contrato de 36 meses oferece o tempo necessário para que o órgão atinja a maturidade operacional e extraia o máximo valor da ferramenta, fortalecendo sua postura de segurança de forma consistente e estratégica.
ü Redução da Carga Administrativa e Foco Estratégico: A gestão de processos de licitação e contratação exige um esforço administrativo considerável da equipe. Optar por um contrato de 36 meses em vez de renovações anuais reduz a carga de trabalho burocrática e operacional. Isso libera a equipe de TI do Tribunal para se dedicar a atividades mais estratégicas e de maior valor para a instituição, como a inovação, o desenvolvimento de projetos e aprimoramentos na infraestrutura tecnológica.

3.5. Equipe de Apoio à Contratação

A equipe de apoio à licitação foi designada formalmente por ato administrativo através da Portaria Nº 077/2024. Caberá à equipe prestar suporte ao pregoeiro, acompanhar a elaboração do edital, responder aos questionamentos durante a fase externa e atuar no julgamento das propostas e habilitações.

3.6. Equipe de Gestão do Contrato

O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderão pelas consequências de sua inexecução total ou parcial.

Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

1. Fiscalização

A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal (is) do contrato, ou pelos respectivos substitutos (Lei nº

14.133/2021, art. 117, caput).

F.1.1 - Fiscalização Técnica
O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (IN CAGE Nº 003/2023, de 2022, art. 10, VI);

O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei 14.133/2021, art. 117, §1º, e IN CAGE Nº 003/2023, de 2022, art. 10, II)

Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 10, III);

O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 10, IV).

No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 10, IV).

O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 10, V).

F.1.2 Gestor do Contrato

O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (IN CAGE Nº 003/2023, de 2022, art. 9, I).

O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (IN CAGE Nº 003/2023, de 2022, art. 9, II).

O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 9, III).

O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 9 VIII).

O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 9 X).

O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Instrução Normativa CAGE Nº 003/2023, de 2022, art. 9 VI).

O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

4. Capítulo 4: Análise de Riscos

A seguir, a análise dos principais riscos mapeados para a contratação da solução de segurança cibernética, com detalhamento das ações de prevenção e contingência.

4.1. Riscos Mapeados

Risco 01: Falha na Implantação da Solução

· Probabilidade: Média

· Impacto: Alto

· Dano: Dispositivos (endpoints e servidores) ficam sem proteção antivírus, gerando vulnerabilidades críticas e possível interrupção de serviços.

· Tratamento: Planejamento e execução de um processo de implantação cauteloso e faseado.

· Ação Preventiva: Realizar a implantação em ambiente de teste e em grupos pequenos de usuários antes de estender a todos os dispositivos.

· Responsável: Setor de Informática.

· Ação de Contingência: Reverter a implantação, desinstalando a solução, e acionar o suporte técnico especializado da contratada para diagnóstico e correção imediata.

· Responsável: Setor de Informática.

Risco 02: Indisponibilidade do Serviço de Gerenciamento

· Probabilidade: Baixa

· Impacto: Alto

· Dano: Perda do controle centralizado sobre a segurança dos dispositivos, impossibilitando atualizações de políticas de segurança e monitoramento de ameaças.

· Tratamento: Garantir que o serviço de gerenciamento tenha alta disponibilidade e suporte adequado.

· Ação Preventiva: Incluir no contrato cláusulas de Nível de Serviço (SLA) que estabeleçam penalidades claras por indisponibilidade, definindo tempos máximos de resposta e correção.

· Responsável: Comissão de Fiscalização.

· Ação de Contingência: Acessar o console de gerenciamento através de rotas alternativas de rede e acionar imediatamente o suporte técnico da contratada, escalando o problema para a liderança.

· Responsável: Setor de Informática.

Risco 03: Obsolescência Tecnológica

· Probabilidade: Média

· Impacto: Alto

· Dano: A solução de segurança contratada se torna incapaz de detectar novas e sofisticadas ameaças, deixando o ambiente de TI vulnerável.

· Tratamento: Assegurar a atualização contínua da tecnologia durante a vigência do contrato.

· Ação Preventiva: O contrato de 36 meses deve garantir acesso a todas as atualizações de software e novas funcionalidades do produto, sem custos adicionais. Acompanhar relatórios de mercado sobre a evolução das ameaças.

· Responsável: Setor de Informática.

· Ação de Contingência: Iniciar, com antecedência, um processo de pesquisa de mercado e planejamento de nova contratação, caso a solução não acompanhe o ritmo das ameaças.

· Responsável: Setor de Informática e Comissão de Licitação.

Risco 04: Falha na Proteção

· Probabilidade: Baixa

· Impacto: Altíssimo

· Dano: O ambiente de TI sofre um incidente grave de segurança (ex: ransomware roubo de dados), comprometendo a operação e a integridade de informações do Tribunal.

· Tratamento: Selecionar e manter uma solução de segurança de ponta e com reputação comprovada no mercado.

· Ação Preventiva: A escolha da solução Kaspersky Next EDR Optimum, que utiliza tecnologia EDR e Inteligência Artificial, minimiza o risco, mas não o elimina completamente.

· Responsável: Setor de Informática.

· Ação de Contingência: Ativar o plano de resposta a incidentes de segurança, isolar os dispositivos afetados, e acionar imediatamente o suporte especializado da Kaspersky para análise forense e remediação.

· Responsável: Equipe de Resposta a Incidentes de Segurança (CSIRT) do Tribunal, grupo específico, dentro ou fora da TIC, treinado para lidar exclusivamente com emergências de segurança cibernética, essa função é frequentemente desempenhada pela própria equipe de Tecnologia da Informação e Comunicação (TIC) do Tribunal. No contexto da análise de riscos, o termo CSIRT foi usado para destacar a necessidade de uma resposta especializada a um incidente.

5. Aprovação e Assinatura

A autoridade competente da área de TIC, com fundamento na justificativa apresentada, nas especificações técnicas constantes neste Estudo Técnico Preliminar e na existência de previsão orçamentária para viabilizar a contratação, aprova o presente ETP e atesta sua conformidade com as disposições da Resolução CNJ nº 468/2022.

Equipe de Planejamento da Contratação**:**

Eduardo de Borba Severo
Coordenador de Tecnologia da Informação e Comunicação - TIC
eduardo-severo@tjmrs.jus.br

Rodrigo Bulloza Gruppelli
Técnico Judiciário
rodrigo-gruppelli@tjmrs.jus.br

Juliana Guglermano Deon Gardin
Servidora
juliana-gardin@tjmrs.jus.br

Documento assinado eletronicamente por **Rodrigo Bulloza Gruppelli**, **Servidor**, em 03/09/2025, às 13:48, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JULIANA GUGLERMANO DEON GARDIN**, **Servidora**, em 03/09/2025, às 13:58, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Eduardo de Borba Severo**, **Coordenador de TIC**, em 03/09/2025, às 15:16, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade deste documento pode ser conferida em https://sei.tjmrs.jus.br/autenticidade, informando o código verificador **0176830** e o código CRC **C660FD69**.