SUBSECRETARIA DE ASSUNTOS ADMINISTRATIVOS

Estudo Técnico Preliminar 143/2025

1. Informações Básicas

Número do processo: 25000.164799/2025-59

2. Descrição da necessidade

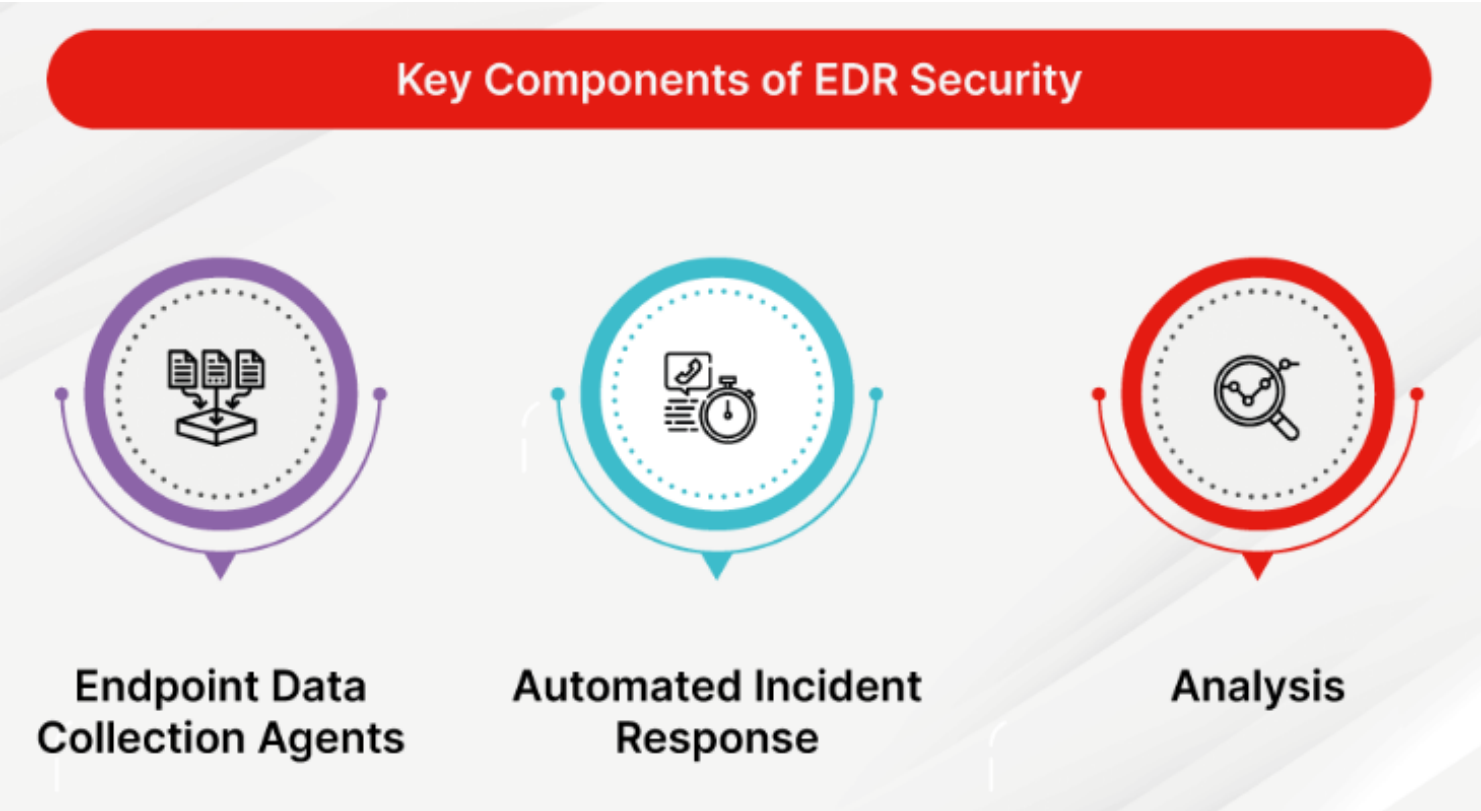
2.1. O presente Estudo Técnico tem por objetivo identificar e analisar os cenários para o atendimento de demanda relacionada ao planejamento para a contratação de solução de Tecnologia da Informação e Comunicação - TIC, a qual tem por objeto a **contratação de subscrição de solução de segurança para proteção de endpoints em estações de trabalho, notebooks e servidores.**

2.2. Em um mundo cada vez mais digital, a segurança cibernética se torna um pilar fundamental para a proteção de dados e sistemas de qualquer organização. As soluções de endpoint assumem um papel crucial nesse cenário, atuando como uma linha de defesa essencial contra as diversas ameaças que surgem constantemente.

2.3. Nesse contexto, os endpoints (estações, notebooks e servidores) constituem os principais vetores de ataque e representam a superfície de risco mais explorada em incidentes de segurança. A ausência de proteção adequada pode comprometer a operação do Ministério da Saúde e causar severos impactos institucionais.

2.4. A segurança de rede permite que sejam interrompidas possíveis ameaças de segurança no nível da rede, bloqueando portas abertas, restringindo o tráfego e empregando serviços de detecção e prevenção de intrusão. A segurança de *endpoints* ajuda a manter seguros os dispositivos que se conectam a uma rede. Ao tornar os *endpoints* o novo perímetro da rede, as organizações podem evitar riscos e detectar atividades suspeitas, não importa onde os funcionários estejam.

2.5. Dito isto, pondera-se que a seleção da solução de segurança certa depende da situação individual e dos requisitos de segurança de cada organização. Fatores importantes a serem incorporados a essa decisão incluem: o número de funcionários, os locais, a propriedade do dispositivo e sensibilidade de dados.



2.6. O Ministério da Saúde possui uma infraestrutura de tecnologia da informação e comunicação (TIC) extensa e crítica, composta por estações de trabalho, notebooks, servidores, sistemas com alta criticidade, bases de dados e serviços de comunicação. Essa infraestrutura é essencial para apoiar a execução de políticas públicas de saúde e garantir o funcionamento contínuo do Sistema Único de Saúde (SUS).

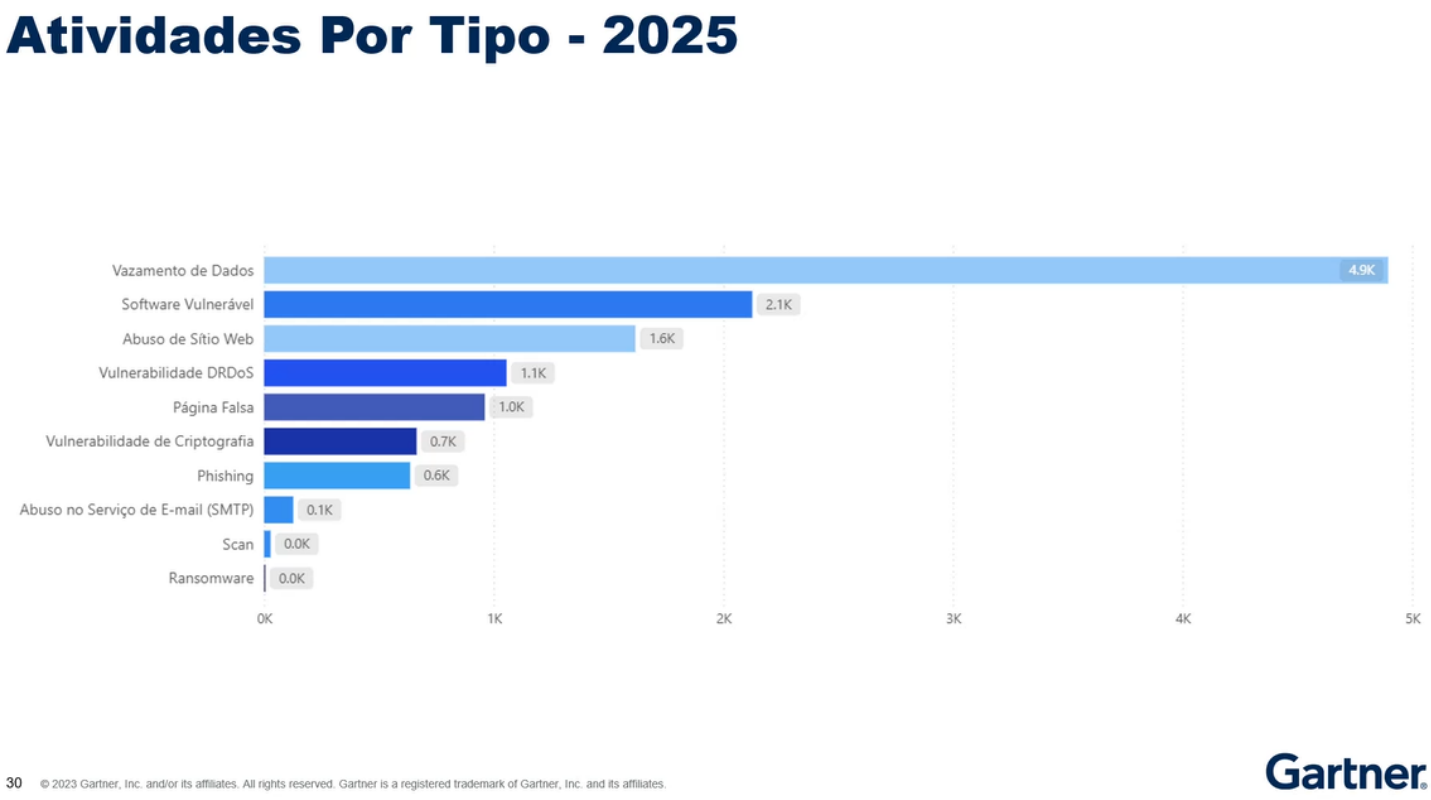
2.7. Vinculado a isto está o fato da informação ser um dos principais ativos da instituição. No entanto, ela está cada vez mais exposta a ameaças cibernéticas, como vírus, *malwares*, ataques de *phishing*, *ransomware* e tentativas de vazamento de dados. Esses incidentes podem comprometer a disponibilidade, integridade, confidencialidade e autenticidade das informações, colocando em risco tanto os serviços prestados à população quanto a imagem institucional do órgão.

2.8. Soluções tradicionais de antivírus não são mais suficientes para mitigar riscos modernos. Há a necessidade de adoção de solução integrada de proteção de endpoints com recursos de inteligência artificial, detecção comportamental, prevenção de exploração e capacidade de resposta a incidentes.

2.9. A solução atualmente utilizada para proteção dos ambientes corporativos é composta por diversas ferramentas da fabricante *Symantec/Broadcom*, responsáveis pela segurança de estações de trabalho, servidores, mensageria eletrônica, armazenamento em rede, gestão de *endpoints* e prevenção contra perda de dados (DLP).

2.10. Contudo, apesar de atender às necessidades atualmente, a solução contratada encontra-se próxima ao vencimento e caso não seja contratada novas subscrições, o ambiente ficará vulnerável e suscetível a ataques cibernéticos, podendo ocasionar a interrupção de serviços essenciais do SUS e a possibilidade de danos permanentes a dados críticos. Além disso, é necessário considerar que o cenário tecnológico e de ameaças evoluiu rapidamente nos últimos anos e a sofisticação dos ataques digitais, aliada à adoção crescente de serviços em nuvem, ao trabalho remoto e à necessidade de conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), impõe a necessidade de modernização e manutenção constante de solução de segurança.

2.11. Segundo a Gartner, empresa global de pesquisa e consultoria em tecnologia da informação (TI) que fornece análises, *insights* e orientação para executivos de negócios tomarem decisões estratégicas, os vazamentos de dados em 2025 serão fortemente influenciados pela Inteligência Artificial Generativa (GenAI), a migração para a nuvem e a crescente superfície de ataque, conforme demonstrado no gráfico a seguir:



https://www.gartner.com.br/pt-br/ciberseguranca/temas/tendencias-em-cibersegurança

2.12. A pesquisa sobre as principais tendências em cibersegurança para 2025 do Gartner constatou uma pressão cada vez maior em relação ao seguinte:

2.12.1. O surgimento contínuo de casos de uso de IA generativa;

2.12.2. O esgotamento mental em decorrência da lacuna permanente entre a oferta e a demanda de talentos em segurança;

2.12.3. O crescimento implacável na adoção da nuvem, que está alterando a composição dos ecossistemas digitais;

2.12.4. O aumento nas obrigações regulatórias e de supervisão governamental na cibersegurança, privacidade e localização de dados;

2.12.5. A descentralização contínua de capacidades digitais em grandes empresas;

2.12.6. O desafio de implantar uma cultura de gestão de riscos colaborativa;

2.12.7. A demanda por estabilidade/segurança nos negócios em um ambiente no qual as ameaças estão em constante evolução;

2.12.8. O bem-estar de CISOs e equipes de segurança;

2.12.9. A gestão colaborativa de riscos cibernéticos; e

2.12.10. A gestão de identidades das máquinas.

2.13. Assim, há necessidade de planejamento para a contratação de solução de proteção de *endpoints* e segurança corporativa, essencial para:

2.13.1. Garantir a continuidade dos serviços de TIC em ambiente seguro;

2.13.2. Elevar o nível de proteção contra ameaças cibernéticas atuais e emergentes;

2.13.3. Atender às exigências legais e regulatórias (LGPD, normas de segurança da informação);

2.13.4. Reduzir riscos de indisponibilidade de serviços críticos e de vazamento de informações sensíveis;

2.13.5. Prover maior governança, visibilidade e gestão centralizada das medidas de segurança; e

2.13.6. Assegurar o alinhamento estratégico às diretrizes institucionais e ao Plano Diretor de TIC.

2.14. Histórico da atual solução implantada no órgão

2.14.1. Em 2016, por meio de adesão à Ata de Registro de Preços nº 09/2016, o Ministério da Saúde realizou a contratação de serviços de Solução de Segurança Integrada e Gerenciamento Seguro para Estações de Trabalho e Ambiente Corporativo. Essa contratação marcou o início da implementação de uma política estruturada de segurança da informação, voltada à proteção do ambiente tecnológico e à mitigação de riscos cibernéticos crescentes;

2.14.2. Posteriormente, com o Contrato Administrativo nº 117/2018, o MS adquiriu licenças adicionais para proteção, segurança e controle de dados da fabricante *Symantec/Broadcom*, complementando o conjunto de soluções de segurança já em uso e promovendo maior integração entre os módulos de proteção;

2.14.3. Essas contratações estabeleceram a base de um portfólio de segurança corporativa integrado, capaz de cobrir de forma ampla os diferentes níveis de risco e os diversos ativos tecnológicos do MS. A combinação das ferramentas implementadas permitiu maior visibilidade, correlação de eventos, resposta automatizada a incidentes e integração entre camadas de defesa, fortalecendo a postura de segurança institucional;

2.14.4. Em novembro de 2021, foi finalizado o planejamento de contratação de solução de segurança, que resultou na Ata de Registro de Preços nº 28/2021, abrangendo os seguintes itens:

- Subscrição *Symantec Endpoint Security Complete* (SESC-SES-CLD-SUB) - responsável pela proteção de estações de trabalho e notebooks, com recursos de antivírus, *firewall*, detecção e resposta a ameaças (EDR) e inteligência em nuvem;
- Subscrição *Symantec Data Center Security* (DCS-SRVA-SUB) - voltada à proteção de servidores físicos e virtuais, garantindo integridade e isolamento de processos críticos;
- Subscrição *Symantec IT Management Suite (Symantec Altiris)* (ALT-SUB) - solução de gerenciamento de *endpoints*, inventário e conformidade, permitindo administração centralizada dos ativos de TIC;
- Subscrição *Symantec Messaging Gateway Hybrid* (SMG-HYB-SUB) - sistema de segurança de mensageria corporativa, com filtros *antispam*, *antimalware* e *antiphishing*, protegendo o e-mail institucional;
- Subscrição *Symantec Data Loss Prevention* (DLP-ES-SUB) - ferramenta de prevenção de perda de dados, que monitora e impede o vazamento de informações sigilosas e dados pessoais, em conformidade com a LGPD; e
- Subscrição *Symantec Protection Engine for NAS* (SPE-NAS-NEW-SUB) - mecanismo de proteção de ambientes de armazenamento em rede (NAS), prevenindo contaminações e garantindo a integridade dos dados compartilhados.

2.14.5. Ato contínuo, após identificação da necessidade de definição do escopo, foi formalizado o **Contrato nº 117/2021**, o qual terá o seu prazo de vigência expirado em 07/12/2026 e o **Contrato nº 102/2022,** que terá seu prazo encerrado em 11/11/2026;

2.14.6. Todas essas soluções foram implementadas de forma planejada e integrada, segundo uma estratégia de portfólio único de segurança, baseada na correlação e retroalimentação de inteligência entre os diferentes módulos, o que se tornou um fator crítico para o sucesso na proteção e resposta a incidentes de segurança cibernética. Essa integração beneficia não apenas as operações de TIC, mas também garante a continuidade dos sistemas críticos do Ministério da Saúde, essenciais para a execução das políticas públicas e para o funcionamento do Sistema Único de Saúde (SUS);

2.14.7. As soluções atualmente em operação são, portanto, fatores estratégicos para o cumprimento da missão institucional do MS, assegurando a proteção de informações sensíveis, a disponibilidade dos serviços e a conformidade com o Programa de Privacidade e Segurança da Informação - PPSI da SGD/MGI, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), e com as diretrizes de governança e segurança da informação da Administração Pública Federal;

2.14.8. Dessa forma, a nova contratação visa garantir a manutenção e evolução das medidas de segurança da informação, assegurando que o MS disponha de ferramentas modernas, integradas e alinhadas às melhores práticas de mercado, essenciais para proteger seus ativos tecnológicos, seus dados e a prestação dos serviços de saúde à população.

2.15. Motivação/Justificativa

2.15.1. O Ministério da Saúde dispõe de um parque tecnológico amplo, heterogêneo e distribuído nacionalmente, responsável por atender milhares de usuários e diversos sistemas críticos do Sistema Único de Saúde (SUS). Atualmente, a infraestrutura é composta por mais de 13 mil estações de trabalho e notebooks, aproximadamente 1.700 servidores físicos e virtuais, 30 mil contas de e-mail corporativo, além de múltiplos data centers, ambientes em nuvem (AWS e Oracle Cloud), sistemas de mensageria e uma rede que interliga milhares de pontos de presença em todo o território nacional;

2.15.2. Esse ecossistema complexo, aliado à criticidade das informações tratadas pelo Ministério da Saúde, torna a área de segurança cibernética estratégica. A informação em saúde é um ativo sensível e de alto valor, sujeito a ameaças como *malwares*, *ransomwares*, *phishing*, acessos não autorizados, vazamento de dados pessoais e ataques direcionados à indisponibilidade de serviços. Tais incidentes podem comprometer a confidencialidade, a integridade e a disponibilidade das informações, impactando diretamente a prestação de serviços à sociedade;

2.15.4. Diante desse cenário, e a crescente necessidade de proteger os dados e a segurança da informação no âmbito da Administração Pública Federal, a Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos - SGD/MGI, criou o Programa de Privacidade e Segurança da Informação - PPSI, por meio da Portaria SGD/MGI nº 852, de 28 de março de 2023, o qual envolve um conjunto de ações de adequação na temática, integrando maturidade, capacidades e resiliência dos órgãos e das entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

2.15.5. Foi publicada recentemente, a Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025, a nova versão do PPSI. O PPSI 2.0 é uma evolução da versão anterior e reforça o compromisso de um Governo confiável e seguro que busca em sua atuação a construção e manutenção da confiança pública, garantindo que os cidadãos possam interagir com o governo de forma segura, promovendo a proteção de direitos, dos dados e das informações.

2.15.6. O framework do PPSI é composto por um conjunto de controles e medidas de privacidade e segurança da informação que devem ser adotadas pelos órgãos e entidades da administração pública federal direta, autárquica e fundacional. Esses controles e medidas estão disponíveis por meio do Guia do Framework de Privacidade e Segurança da Informação link: https://www.gov.br /governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/. Este guia apresenta a importância de cada controle proposto no framework, incluindo diretrizes que auxiliam as organizações desde a gestão básica até a implementação operacional das medidas, promovendo a conformidade, a maturidade e a resiliência dos órgãos nos aspectos relacionados à privacidade e segurança da informação.

2.15.7. Dito isto, o guia apresenta controles de governança, segurança da informação e privacidade. Dentre eles, podemos destacar os que tratam de segurança da informação, o qual consiste em um conjunto recomendado de melhores práticas priorizadas de defesa cibernética. Elas fornecem ações específicas e práticas de proteção contra os ataques mais difundidos e críticos da atualidade. Abaixo apresentamos uma explanação de alguns controles que envolvem o presente estudo:

- **Controle 1 - Inventário de ativos institucionais**

  Visão geral:

  Gerenciar ativamente (inventariar, rastrear e corrigir) todos os ativos institucionais (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais/IoT e servidores) conectados à infraestrutura fisicamente, virtualmente ou remotamente e aqueles dentro de ambientes de nuvem, para conhecer com precisão a totalidade dos ativos que precisam ser monitorados e protegidos na organização. Isso também ajudará a identificar ativos não autorizados e não gerenciados objetivando remoção ou remediação.

  Por que esse controle é crítico?

A organização não pode defender o que não sabe que possui. O controle gerenciado de todos os ativos institucionais também desempenha um papel crítico no monitoramento de segurança, resposta a incidentes, backup e recuperação de sistemas. As organizações devem saber quais dados são críticos para elas, e o gerenciamento adequado de ativos institucionais ajudará a identificar quais contêm ou gerenciam esses dados críticos, para que os controles de segurança apropriados possam ser aplicados. Ativos adicionais que se conectam à rede da organização (por exemplo, sistemas de demonstração, sistemas de teste temporários, redes de convidados) devem ser identificados e/ou isolados para evitar que o acesso adversário afete a segurança das operações da organização.

Além disso, dispositivos portáteis de usuários finais se conectam periodicamente à rede e depois desaparecem, tornando o inventário de ativos desafiador neste cenário dinâmico. Da mesma forma, ambientes de nuvem e máquinas virtuais podem ser difíceis de rastrear em inventários de ativos quando estão desligados ou pausados. Manter uma visão atualizada e precisa dos ativos é um processo contínuo e dinâmico.

Procedimentos e ferramentas

Este controle requer ações técnicas e procedimentais, unidas em uma estratégia para promover o gerenciamento do inventário de ativos institucionais. Para auxiliar na implementação deste controle, as organizações podem aproveitar ferramentas de segurança já instaladas em ativos institucionais ou usadas na rede, incluindo tecnologias para varredura de descoberta da rede com um scanner de vulnerabilidades, revisar logs antimalware, logs de portais de segurança de endpoint, logs de rede de switches ou logs de autenticação e gerenciar os resultados em uma planilha ou banco de dados. Mesmo para pequenas organizações, raramente há uma única fonte para realizar o inventário de ativos institucionais, pois nem sempre os ativos são provisionados pelo departamento de TI. A realidade é que diversas fontes precisam ser consideradas para se ter um inventário de alta confiabilidade. Organizações mais complexas podem adotar produtos mais abrangentes e de larga escala. Além das fontes de ativos mencionadas acima para pequenas organizações, as maiores podem coletar dados de portais e logs em nuvem de plataformas organizacionais, como: Active Directory (AD), Single Sign-On (SSO), Autenticação Multifator (MFA), Rede Privada Virtual (VPN), Sistemas de Detecção de Intrusão (IDS) ou Inspeção Profunda de Pacotes (DPI), Gerenciamento de Dispositivos Móveis (MDM) e ferramentas de varredura de vulnerabilidades. Existem ferramentas e métodos que normalizam esses dados para identificar dispositivos que são únicos entre essas fontes.

- **Controle 3: Proteção de dados**

  Visão geral

  Aplicar processos e controles técnicos para identificar, categorizar, utilizar, reter e descartar dados com segurança, garantindo a proteção dos dados ao longo de todo o seu ciclo de vida.

  Por que esse controle é crítico?

  Os dados ultrapassam os limites da organização, estando na nuvem, nas casas dos agentes públicos, em dispositivos portáteis e compartilhados com parceiros, o que demanda gestão e proteções adequadas ao longo de todo o ciclo de vida dos dados, incluindo aspectos de conformidade. Além dos dados críticos para as estratégias dos diferentes órgãos, existem dados relacionados a finanças, propriedade intelectual e dados de cidadãos custodiados pela organização. Invasores buscam extrair esses dados confidenciais, mas muitas organizações não monitoram o tráfego de saída, ficando vulneráveis. Além de ataques na rede, há riscos como roubo físico de dispositivos e ameaças à parceiros que armazenam esses dados. A perda de controle sobre esses dados gera impactos graves, muitas vezes decorrentes de má gestão e erros humanos.

  Procedimentos e ferramentas

  É fundamental que a organização estabeleça um processo de gerenciamento de dados com diretrizes para categorização, proteção, manuseio, retenção e descarte. Também deve haver um processo para tratar possíveis violações de dados que se integre ao plano de resposta a incidentes e aos planos de conformidade e comunicação. Os dados devem ser categorizados considerando os diferentes níveis de criticidade. Em seguida, criar um inventário que mapeie os dados, os softwares que os acessam e os ativos que os hospedam. A rede deve ser segmentada conforme níveis de criticidade, considerando a utilização de firewalls ou outros recursos tecnológicos para controlar o acesso a cada segmento e aplicando regras de acesso de usuários para permitir o acesso aos dados apenas àqueles que realmente necessitam.

- **Controle 7: Proteção de dados**

  Visão geral

Desenvolver um plano para avaliar e monitorar continuamente vulnerabilidades em todos os ativos de informação da organização, a fim de remediar e minimizar a janela de oportunidade para atacantes. Monitorar fontes públicas e privadas em busca de novas informações sobre ameaças e vulnerabilidades.

Por que esse controle é crítico?

Vulnerabilidades são alvo constante de atacantes. As equipes de segurança devem acompanhar de forma ágil informações sobre: atualizações de soluções software, patches, alertas de segurança, boletins de ameaças, entre outros, e devem revisar regularmente seu ambiente para identificar vulnerabilidades antes que os invasores o façam. Vulnerabilidades novas ou desconhecidas ("zero-day") aumentam o risco e as equipes precisam estar ciente desta possibilidade pois podem precisar implementar outros controles para mitigar o risco. As organizações que não avaliam sua infraestrutura em busca de vulnerabilidades e não abordam proativamente as falhas descobertas enfrentam uma probabilidade significativa de ter seus ativos de informação comprometidos. Sem gestão contínua, o ambiente fica vulnerável a explorações.

Procedimentos e ferramentas

Planos documentados para gestão de vulnerabilidades são necessários. Ferramentas de varredura automatizada, tanto autenticada quanto não autenticada, devem ser usadas regularmente para identificar vulnerabilidades internas e externas. Para ajudar a padronizar as definições de vulnerabilidades descobertas em uma organização, é preferível usar ferramentas de varredura de vulnerabilidades que mapeiem vulnerabilidades para um ou mais dos seguintes esquemas e linguagens de classificação de vulnerabilidades, configurações e plataformas especificadas na publicação NIST SP 800-126r32: Common Vulnerabilities and Exposures (CVE®), Common Configuration Enumeration (CCE), Open Vulnerability and Assessment Language (OVAL®), Common Platform Enumeration (CPE), Common Vulnerability Scoring System (CVSS) ou Extensible Configuration Checklist Description Format (XCCDF). A remediação deve ser priorizada e executada conforme os riscos. Além das varreduras, outras ferramentas analisam configurações de segurança e identificam mudanças não autorizadas ou vulnerabilidades introduzidas inadvertidamente. Organizações eficientes conectam scanners a sistemas de emissão de tickets para acompanhar a correção de vulnerabilidades e reportar à alta gerência, permitindo priorização e cumprimento de requisitos de conformidade.

Deve haver um processo de garantia de qualidade para verificar se as atualizações de configuração ou se os patches foram implementados corretamente em todos os ativos institucionais relevantes.

- **Controle 9: Proteção de e-mail e navegador web**

Visão geral

Aprimorar as proteções e detecções de ameaças provenientes de e-mails e da web, pois essas são oportunidades para invasores manipularem o comportamento humano por meio de diferentes técnicas.

Por que esse controle é crítico?

E-mail e navegadores web são vetores comuns para diferentes tipos de ataques, incluindo engenharia social e malware, pois estão diretamente expostos aos usuários. Malwares exploram vulnerabilidades de navegadores e suas extensões. Por sua vez, os e-mails são os principais canais para phishing, impactando a segurança das organizações.

Procedimentos e ferramentas

Manter apenas versões suportadas pelos seus fabricantes de navegadores (incluindo suas extensões) e clientes de e-mail. Restringir extensões não autorizadas e de fontes não confiáveis. Usar filtros DNS nativos dos navegadores para bloquear sites maliciosos, além de filtros de URL na rede. Considerar também a assinatura de serviços de filtragem de DNS para bloquear tentativas de acesso. Implementar filtragem de spam e verificação de malware no gateway de e-mail, bem como Domain-Based Message Authentication, Reporting, and Conformance (DMARC), ajuda a reduzir atividades de spam e phishing. Além de filtros com base no remetente, recomenda-se bloquear tipos de arquivos não necessários no gateway de e-mail. A instalação de uma ferramenta de criptografia para proteger e-mails e comunicações adiciona outra camada de segurança para o usuário e para a rede. Proteções de antivírus e sandboxing para servidores de e-mail também são fatores que auxiliam na mitigação do risco. Como os ataques de phishing por e-mail evoluem constantemente para burlar os filtros de spam, antivírus, sandboxing e demais medidas técnicas de segurança da informação, é fundamental conscientizar os agentes públicos para que saibam identificar mensagens suspeitas e as reportem à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR). Realizar simulações regulares de phishing é uma prática eficaz para conscientizar os agentes públicos, ajudando-os a reconhecer diferentes tipos de ataques e a acompanhar a evolução dessas ameaças ao longo do tempo.

- **Controle 10: Defesa contra malware**

Visão geral

Prevenir a instalação, disseminação e execução de aplicativos, códigos ou scripts maliciosos em ativos institucionais.

Por que esse controle é crítico?

Software maliciosos são uma ameaça constante, com finalidades diversas como captura de credenciais, roubo e destruição de dados. O malware evolui usando técnicas como aprendizado de máquina para evitar ou desabilitar defesas. Ele entra nas organizações por vulnerabilidades em dispositivos de usuários finais, anexos de e-mail, páginas web, serviços em nuvem, dispositivos móveis e mídias removíveis, explorando comportamentos inseguros como clicar em links, abrir anexos ou usar pen drives USB. As defesas contra malware devem operar de forma automatizada, atualizada rapidamente e integradas a processos como gerenciamento de vulnerabilidades e gestão de incidentes, sendo implantadas em todos os pontos de entrada e ativos institucionais para detectar, impedir a disseminação e controlar a execução do código malicioso.

Procedimentos e ferramentas

A proteção eficaz contra malware inclui suítes tradicionais de prevenção e detecção em endpoints, com atualizações automatizadas dos fornecedores para manter os Indicadores de Comprometimento (IOCs) atualizados. Essas ferramentas devem ser gerenciadas centralizadamente para garantir consistência em toda a infraestrutura. Além de bloquear e identificar malware, este controle destaca a importância da coleta centralizada de logs para suportar alertas, identificação e resposta a incidentes. Invasores utilizam técnicas Living Off The Land (LotL), empregando recursos já existentes no ambiente para evitar detecção. Habilitar o registro em log facilita o acompanhamento e a compreensão dos eventos de segurança – o controle 13 apresenta medidas detalhadas nesta perspectiva.

2.15.8. Como podemos verificar, as soluções de segurança em uso no MS são instrumentos fundamentais e compatíveis com diversos controles e objetivos do PPSI 2.0, especialmente no eixo de tecnologia e nos controles de cibersegurança e proteção de dados. Quando bem implementadas e acompanhadas de governança, processos e monitoramento, permitem que o órgão atenda aos requisitos de segurança da informação e privacidade impostos pelo programa.

2.15.9. A solução atualmente utilizada, baseada em uma solução integrada da fabricante *Symantec/Broadcom*, tem garantido a proteção de *endpoints*, servidores, mensageria eletrônica, prevenção contra perda de dados (DLP), controle de ativos e segurança de armazenamento em rede. Entretanto, o contrato vigente encontra-se em fase final de vigência, com término previsto para o segundo semestre de 2026. A não renovação ou substituição tempestiva dessa solução acarretaria grande exposição a riscos, considerando a impossibilidade de manter atualizações, suporte técnico e continuidade de cobertura contra ameaças cibernéticas;

2.15.10. A proteção de *endpoints* é essencial porque são os equipamentos diretamente utilizados pelos servidores e colaboradores do Ministério da Saúde. Neles estão armazenadas informações sensíveis, além de serem a porta de entrada mais comum para ataques cibernéticos por meio de arquivos, navegação na internet ou e-mails maliciosos;

2.15.11. A proteção de servidores é igualmente crítica, pois esses ativos concentram sistemas corporativos, bancos de dados e aplicações que sustentam o funcionamento do SUS. Um ataque ou indisponibilidade em servidores pode comprometer serviços de saúde em âmbito nacional, impactando diretamente cidadãos e profissionais da área;

2.15.12. A proteção da mensageria eletrônica (e-mail corporativo) é necessária porque esse é um dos principais canais de comunicação institucional e um dos vetores mais explorados por criminosos digitais. Mensagens falsas ou maliciosas podem veicular vírus, aplicar golpes *(phishing)* e ser utilizadas como porta de entrada para ataques mais complexos;

2.15.13. A prevenção contra perda de dados (DLP) é indispensável para evitar que informações estratégicas e dados pessoais sensíveis sejam divulgados ou acessados de forma indevida. Isso garante conformidade com a LGPD, preserva a confidencialidade das informações de saúde e evita danos à imagem institucional;

2.15.14. O controle de ativos é necessário porque o parque tecnológico do Ministério é vasto e distribuído por todo o país. A falta de visibilidade e gerenciamento desses ativos pode gerar falhas de segurança, dificultar a aplicação de políticas de proteção e aumentar a vulnerabilidade a incidentes;

2.15.15. A adoção combinada de soluções (endpoint + data center + DLP + gateway + gestão) cobre diversas camadas de defesa — desde estações de trabalho até servidores, comunicação e dados — fortalecendo a maturidade de segurança, conforme os eixos “Tecnologia” e “Governança” do PPSI.

2.15.16. Assim, a proteção integrada de *endpoints*, servidores, mensageria eletrônica, prevenção contra perda de dados, controle de ativos e armazenamento em rede é indispensável para garantir a continuidade dos serviços, a confidencialidade e a integridade das informações do Ministério da Saúde, assegurando a confiança da sociedade nos serviços prestados;

2.15.17. Portanto, a motivação para a contratação decorre da necessidade de:

- Garantir a continuidade da proteção de *endpoints*, servidores e serviços críticos;
- Avaliar a necessidade de modernizar a solução, incorporando recursos alinhados ao atual cenário de ameaças e boas práticas de mercado;

- Prover mecanismos de segurança capazes de atuar em ambientes híbridos (*on-premises* e nuvem);
- Atender às exigências de governança, conformidade e LGPD; e
- Sustentar a infraestrutura tecnológica do Ministério da Saúde, assegurando a resiliência cibernética necessária ao pleno funcionamento do SUS.

2.16. O objeto da contratação está previsto no Plano de Contratações Anual de 2026, conforme consta das informações básicas deste Estudo Técnico Preliminar.

ALINHAMENTO PCA 2026					
DFD nº	**Item**	**Descrição**	**Unidade de Medida**	**Quantidade**	**CATSER**
272/2025	01	Cessão temporária de direitos sobre programas de computador locação de software.	Unidade	15.061	27502
	02	Cessão temporária de direitos sobre programas de computador locação de software.	Unidade	353	27502
	03	Cessão temporária de direitos sobre programas de computador locação de software.	Unidade	15.061	27502
	04	Cessão temporária de direitos sobre programas de computador locação de software.	Unidade	22.826	27502
	05	Cessão temporária de direitos sobre programas de computador locação de software.	Unidade	15.061	27502

2.17. O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2024 a 2027 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2022-2024 do Ministério da Saúde, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS		
ID	**OBJETIVOS ESTRATÉGICOS**	**NOME DO DOCUMENTO**
Diretiva 8. Segurança da Informação	Políticas, planos e normas que abrangem a segurança e defesa cibernética, a segurança física e a proteção de dados e demais ativos organizacionais; compreende um conjunto de ações técnicas, gerenciais e institucionais destinadas a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.	**PDTIC 2022-2024**
OE.11	Aprimorar e preservar a segurança das informações digitais sob a custódia do Ministério da Saúde.	
N156	*Protect by design:* Desenvolvimento seguro, Arquitetura de infraestrutura segura e *Observability* nos dados.	

ALINHAMENTO AO PDTIC 2022-2024*			
ID	**AÇÃO DO PDTIC**	**ID**	**META DO PDTIC ASSOCIADA**
A41.5	Contratar solução de segurança e proteção de *endpoint*.	**M.41**	Contratações realizadas.

* Cabe destacar que o novo PDTIC 2026–2028 encontra-se em fase de elaboração e, em razão dessa circunstância, o PDTIC 2022-2024 foi formalmente prorrogado por mais 12 (doze) meses, conforme decisão do Comitê de Governança Digital (CGD), deliberada em reunião realizada em 14/07/2025 e registrada no Processo SEI nº 25000.126447/2022-52.

3. Área requisitante

Área Requisitante	Responsável
Coordenação-Geral de Infraestrutura e Segurança da Informação - CGIE	Ramon Moreno de Matos Vieira
Coordenação de Segurança da Informação - COSEGI	Marcelo Dias de Sá

4. Necessidades de Negócio

4.1. Apontam-se as necessidades de negócio que serão atendidas com a proposta de solução a ser desenvolvida neste Estudo:

4.1.1. Garantir a proteção de estações de trabalho, notebooks e servidores, contra vírus, *malwares*, *ransomwares* e outras ameaças cibernéticas;

4.1.2. Assegurar a proteção do correio eletrônico institucional, com recursos de filtragem *antispam*, *antiphishing* e *antimalware*, evitando golpes e contaminações via e-mail;

4.1.3. Prevenir o vazamento de informações sigilosas e dados pessoais sensíveis, em conformidade com a LGPD, por meio de mecanismos de monitoramento e bloqueio de tentativas não autorizadas;

4.1.4. Oferecer gestão centralizada e visibilidade completa sobre o estado de segurança de todos os ativos do parque tecnológico (estações, servidores, dispositivos móveis e ambientes em nuvem);

4.1.5. Disponibilizar recursos de resposta e investigação de incidentes, que permitam identificar, conter e remediar ameaças de forma ágil e eficiente;

4.1.6. Assegurar proteção também em ambientes híbridos, contemplando infraestrutura local *(on-premises)*, nuvem pública e modelos de trabalho remoto;

4.1.7. Garantir escalabilidade da solução, de modo a suportar a evolução e o crescimento do parque tecnológico do Ministério da Saúde;

4.1.8. Disponibilizar relatórios e indicadores de segurança, que apoiem a tomada de decisão, a gestão de riscos e a prestação de contas à alta administração;

4.1.9. Atender às normas, políticas e legislações vigentes, em especial a LGPD, ao Programa de Privacidade e Segurança da Informação - PPSI 2.0, a Política de Gestão de Riscos do Ministério da Saúde, a Política de Segurança da Informação do MS e as diretrizes do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC);

4.1.10. Possibilitar suporte técnico contínuo e atualização de assinaturas e bases de proteção, assegurando que a solução se mantenha eficaz contra novas ameaças; e

4.1.11. Garantir a padronização em todos os dispositivos corporativos por meio da gestão centralizada.

5. Necessidades Tecnológicas

5.1. A partir da análise das necessidades de negócio, identificaram-se as necessidades tecnológicas a serem atendidas pela solução, conforme requisitos elencados nos itens a seguir:

5.1.1. A solução deverá ser composta por módulos integrados, reduzindo o risco decorrentes de soluções fragmentadas ou não integradas;

5.1.2. Prevenir, detectar e responder a ameaças cibernéticas, incluindo malwares, ransomwares, spywares, exploits, ataques de dia zero e ameaças persistentes avançadas;

5.1.3. Utilizar mecanismos modernos de detecção, como análise comportamental, heurística, aprendizado de máquina e inteligência artificial;

5.1.4. Permitir resposta automatizada a incidentes, incluindo isolamento do endpoint, bloqueio de processos maliciosos e mitigação de danos;

5.1.5. Proteger contra ataques baseados em memória e exploração de vulnerabilidades;

5.1.6. Operar de forma contínua, mesmo em situações de conectividade limitada;

5.1.7. Ser compatível com os sistemas operacionais utilizados no ambiente institucional;

5.1.8. Possuir proteção para servidores físicos e virtuais, bem como workloads executados em ambientes de nuvem pública, privada ou híbrida;

5.1.9. Mecanismos de proteção antimalware e anti-exploit adequados a ambientes de missão crítica;

5.1.10. Detecção de comportamentos anômalos e tentativas de escalonamento indevido de privilégios;

5.1.11. Visibilidade centralizada do estado de segurança dos servidores, com alertas e registros de eventos;

5.1.12. Inventário automatizado de hardware e software;

5.1.13. Monitoramento do estado de conformidade e segurança dos ativos;

5.1.14. Distribuição, atualização e gerenciamento remoto dos agentes e políticas de segurança;

5.1.15. Mecanismos de antispam, antiphishing, antimalware e antifraude;

5.1.16. Aplicação de políticas de segurança em ambientes locais, em nuvem ou híbridos;

5.1.17. Geração de relatórios técnicos e gerenciais que subsidiem a tomada de decisão;

5.1.18. Identificar, classificar e proteger informações sensíveis, pessoais ou estratégicas;

5.1.19. Monitorar e controlar a movimentação de dados em endpoints, servidores, correio eletrônico e outros canais;

5.1.20. Gerar registros, alertas e evidências para fins de auditoria e apuração;

5.1.21. Apoiar a conformidade com legislações e normativos aplicáveis, como a Lei Geral de Proteção de Dados Pessoais (LGPD).

5.1.22. Correlação de eventos e resposta coordenada a incidentes de segurança;

5.1.23. Contar com suporte técnico especializado e atualizações contínuas; e

5.1.24. Estar aderente as boas práticas, normas e padrões de segurança da informação.

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

6.1. Além dos requisitos de negócio e tecnológicos apresentados neste Estudo, a presente seção destaca aqueles requisitos que devem ser considerados para assegurar o alcance dos objetivos pretendidos com a contratação em tela, de forma que a solução deverá:

6.1.1. Funcionar com eficiência e eficácia em regime integral, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do mês, em perfeitas condições;

6.1.2. Deverá ser escalável, suportando crescimento do parque tecnológico sem degradação significativa de desempenho;

6.1.3. Facilidade de instalação, configuração e manutenção remota;

6.1.4. Atualizações automáticas e seguras de assinaturas e módulos;

6.1.5. Os agentes instalados em endpoints e servidores deverão apresentar baixo impacto no desempenho, especialmente em ambientes críticos;

6.1.6. Compatibilidade com a política de *proxy*, *VPN* e *firewall* da instituição; e

6.1.7.O fornecedor deverá demonstrar capacidade de evolução tecnológica, acompanhando novas ameaças e vetores de ataque.

6.1.8. Deverá manter trilhas de auditoria completas, registrando ações administrativas, eventos de segurança e incidentes.

6.2. Sustentabilidade:

6.2.1. A solução deve contribuir para a redução de impactos ambientais, especialmente relacionados ao consumo de energia, resíduos eletrônicos e otimização do ciclo de vida de equipamentos;

6.2.2. A solução deve apresentar baixo consumo de recursos computacionais, de modo a reduzir o consumo energético e prolongar a vida útil de estações de trabalho e servidores; e

6.2.3. Deverá minimizar a necessidade de infraestrutura adicional dedicada, privilegiando arquiteturas otimizadas, virtualizadas ou em nuvem, quando aplicável.

6.2.4. A solução deverá contribuir para a eficiência do gasto público, em consonância com o interesse público.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. Características da Solução Atual

7.1.1. Em 2021, foi realizada contratação visando à escolha da proposta mais vantajosa para o Registro de preços para contratação de solução integrada de segurança para estação de trabalho e servidores em ambiente corporativo, da qual resultou a Ata de Registro de Preços nº 28/2021, oriunda do Pregão Eletrônico nº 34/2021, conforme detalhado na tabela a seguir:

Razão Social: BLUE EYE SOLUCOES EM TECNOLOGIA LTDA

CNPJ/MF: 26.025.401/0001-90

Endereço: SHN Quadra 01, Conjunto A, Bloco D, Entrada A, Salas 1503 e 1504

Edifício Fusion Work e Live, Asa Norte - Brasília/DF - CEP 70701-040

Telefone: (61) 3038-1127 - (61) 98195-0705 | E-mail: comercial@blueeye.com.br

Representante: Rinaldo Araújo da Silva

Grupo	Item	Descrição/ Especificação	Part Number/ SKU	Identificador	Unidade de Medida	Requisição		Quantidade Total	Valores (R$)	
						Mínima	Máxima		Unitário	Total
1	1	Subscrição Symantec Endpoint Security Complete	SESC-SES-CLD-SUB	Endpoint Security Complete (Includes New SES/SEP Subscription), Hybrid Subscription License with Support, Per Device, 1Y	Unidade	55	20.100	20.155	153,00	3.083.715,00
	2	Subscrição Symantec Data Center Security	DCS-SRVA-SUB	Data Center Security Server Advanced, Subscription License with Support, Per Server, 1Y	Unidade	10	1.900	2.000	221,00	442.000,00
	3	Subscrição Symantec It Management Suíte (Symantec Altiris)	ALT-SUB	Altiris Client Management Suite, Subscription License with Support, Per Server, 1Y	Unidade	9	16.940	16.949	145,00	2.457.605,00
	4	Subscrição Symantec Messaging Gateway Hybrid	SMG-HYB-SUB	Symantec Messaging Gateway Hybrid Advanced, Subscription License with Support, 1 YR	Unidade	40	20.200	20.240	65,75	1.330.780,00
	5	Subscrição Symantec Data Loss Prevention	DLP-ES-SUB	Data Loss Prevention Enterprise Suite, Subscription License with Support, 1 YR	Unidade	40	20.200	20.240	201,00	4.068.240,00
	6	Subscrição Symantec Protection Engine for NAS	SPE-NAS-NEW-SUB	Protection Engine for NAS, Subscription License with Support, 1YR	Unidade	5	3.995	4.000	30,00	120.000,00
									VALOR TOTAL	**11.502.340,00**

7.1.2. Em sequência, foi formalizado o **Contrato nº 117/2021, vigente até o dia 07/12/2026**, para o fornecimento da solução integrada de segurança para estação de trabalho e servidores em ambiente corporativo, com o seguinte escopo:

Grupo	Item	Descrição do Serviço	Valor Unitário (R$)	Quantidade a ser Contratada	Valor Total (R$)
1	1	Subscrição *Symantec Endpoint Security Complete*	153,00	15.474	**2.367.522,00**
	2	Subscrição *Symantec Data Center Security*	221,00	900	**198.900,00**
	3	Subscrição *Symantec It Management Suíte (Symantec Altiris)*	145,00	15.474	**2.243.730,00**
	4	Subscrição *Symantec Messaging Gateway Hybrid*	65,75	15.474	**1.017.415,50**
	5	Subscrição *Symantec Data Loss Prevention*	201,00	40	**8.040,00**
	VALOR TOTAL (R$)				**5.835.607,50**

7.1.3. Atualmente, o referido Contrato encontra-se em seu Quarto Termo Aditivo, conforme escopo e valores apresentados abaixo:

Item	Especificação	Quantidade	Valor unitário Reajustado (R$)	Valor Total Reajustado (R$)
1	Subscrição Symantec Endpoint Security Complete	15.474	174,85	2.705.628,90
2	Subscrição *Symantec Data Center Security*	900	243,78	219.402,00
3	Subscrição *Symantec It Management Suíte (Symantec Altiris)*	15.474	165,71	2.564.196,54
4	Subscrição *Symantec Messaging Gateway Hybrid*	15.474	75,13	1.162.561,62
5	Subscrição *Symantec Data Loss Prevention*	40	229,72	9.188,80
VALOR TOTAL (R$)				**6.660.977,86**

7.1.4. Adicionalmente, foi formalizado também o **Contrato nº 102/2022, vigente até o dia 11/11/2027**, com o seguinte escopo:

Grupo	Item	Descrição do Serviço	Quantidade a ser Contratada	Valor Unitário (R$)	Valor Total (R$)
1	4	Subscrição *Symantec Messaging Gateway Hybrid*	4.681	65,75	307.775,75
	5	Subscrição *Symantec Data Loss Prevention*	20.200	201,00	4.060.200,00
	VALOR TOTAL (R$)				**4.367.975,75**

7.1.5. No que se refere ao Contrato nº 102/2022, este encontra-se atualmente em seu Terceiro Termo Aditivo, conforme detalhamento a seguir:

Grupo	Item	Descrição do Serviço	Quantidade	Valor Unitário (R$)	Valor Total (R$)
1	4	Subscrição *Symantec Messaging Gateway Hybrid*	4.681	75,13	351.683,53
	5	Subscrição *Symantec Data Loss Prevention*	20.200	229,72	4.640.344,00
	VALOR TOTAL (R$)				**4.992.027,53**

7.1.6. Considerando o prazo de vigência dos contratos atuais, e a necessidade de continuidade dos serviços, foi realizado o levantamento das licenças disponíveis na console de gerenciamento das subscrições, conforme Relatório anexado ao processo SEI nº 0051504112:

7.1.6.1. **Item 1 - Subscrição *Symantec Endpoint Security Complete* (SESC):** solução integrada de proteção avançada para estações de trabalho, servidores e dispositivos móveis. Ela combina antivírus de última geração, prevenção contra intrusões (IPS), controle de aplicações, *firewall*, inteligência comportamental e resposta a incidentes, tudo gerenciado de forma centralizada. Atualmente, com os seguintes quantitativos em utilização:

- Quantidade de licenças contratadas: 15.474.

7.1.6.2. **Item 2 - Subscrição *Symantec Data Center Security (DCS)*:** solução de proteção e controle de segurança para servidores físicos, virtuais e ambientes de nuvem, projetada para prevenir alterações não autorizadas, bloquear explorações e garantir conformidade de *workloads* críticos, com a seguinte utilização:

- Quantidade de licenças contratadas: 900.

7.1.6.3. **Item 3 - Subscrição *Symantec IT Management Suite (Altiris)*:** plataforma de gerenciamento centralizado de ativos e *endpoints* que permite inventariar, provisionar, configurar, atualizar e controlar estações de trabalho, notebooks e servidores em larga escala, com a seguinte utilização:

- Quantidade de licenças contratadas: 15.474.

7.1.6.4. **Item 4 - *Symantec Messaging Gateway Hybrid*:** solução de segurança de e-mail baseada em nuvem que protege domínios corporativos contra *spam*, *phishing*, *malware*, *ransomware* e ataques avançados, antes das mensagens chegarem ao ambiente interno, com o seguinte status de utilização:

- Quantidade de licenciamento contratado: 15.474;

7.1.6.5. **Item 5 - *Symantec Data Loss Prevention:*** solução de Email Security em nuvem *(antispam)* permanece operando normalmente, mesmo quando o limite de licenciamento é excedido, com o seguinte status de utilização:

- Quantidade de licenças contratadas: 20.240;

7.2. Estudo para a Estimativa da Demanda

7.2.1. Para definição do quantitativo estimado da contratação, inicialmente foi realizado o levantamento das mudanças de cenário do MS ocorridas no decorrer dos últimos anos. Nesse contexto, destaca-se o processo de descentralização dos Hospitais Federais do Rio de Janeiro - HFRJ para as prefeituras, iniciado em 2024, conforme o processo SEI nº 25000.173725/2024-22, por meio das portarias a seguir:

7.2.1.1. Portaria GM/MS Nº 4.847, de 5 de julho de 2024, a qual estabelece a descentralização dos serviços do Hospital do Andaraí, órgão público federal, para a Prefeitura Municipal do Rio de Janeiro;

7.2.1.2. Portaria GM/MS nº5.415, de 14 de Outubro de 2024, a qual dispõe sobre a descentralização dos serviços de saúde do Hospital Federal do Bonsucesso para a Empresa Pública Nossa Senhora da Conceição S.A, dominado Grupo Hospital Conceição-GHC;

7.2.1.3. Portaria GM/MS n 5.817, de 4 de dezembro de 2024, a qual estabelece a descentralização dos serviços do Hospital de Cardoso Fontes, órgão público federal, para a Prefeitura Municipal do Rio de Janeiro.

7.2.2. Ressalta-se que, até o momento, apenas a transição do Hospital de Cardoso Fontes foi concluída. Assim, os demais hospitais serão considerados para fins de estimativa da demanda.

7.2.3. Diante disso, para a estimativa da quantidade de licenças, foi realizado o levantamento das quantidades de ativos, usuários e localidades a serem atendidas. Para tanto, foi solicitada à Coordenação de Gestão de Redes e Datacenter - COGRD a realização de levantamento atualizado do parque.

7.2.4. Com base no levantamento realizado, anexado aos autos SEI nº 0051633355, segue abaixo o memorial de cálculo para estimativa do quantitativo de subscrições:

Memorial de Cálculo para a definição do quantitativo de licenças para o Ministério da Saúde					
Localidade	**Quantidade de Usuários**	**Quantidade de Desktops**	**Quantidade de Notebooks**	**Servidores**	
				Desenvolvimento e Homologação	**Críticos**

Ministério da Saúde-Sede	15.411	9.864	647	180	496
Hospital Federal de Bom Sucesso	2.807	1.262	10	9	56
Hospital Federal de Ipanema	965	874	1	6	41
Hospital Federal da Lagoa	1.290	614	6	4	42
Hospital Federal dos Servidores do Estado	1.675	1.106	29	6	58
Ministério da Saúde-RJ	678	623	25	115	581
Quantidade Total	**22.826**	**14.343**	**718**	**320**	**1.274**

7.3. Método adotado para o cálculo das estimativas das quantidades dos itens a contratar:

7.3.1. Para definição do quantitativo, considerando a destinação de cada solução pretendida foi realizada da seguinte forma:

Estimativa da demanda - memória de cálculo							
Tipo	**Unidade de medida utilizada para definição do quantitativo**	**Quantidade de Usuários**	**Quantidade Total de de Desktops**	**Quantidade de Notebooks**	**Servidores**		**Quantidade Total por item**
					Desenvolvimento e Homologação	**Críticos**	
Proteção avançada de endpoints	por máquina	-	14.343	718	-	-	**15.061**
Proteção de servidores físicos, virtuais e ambientes em nuvem	por máquina	-	-	-	-	353	**353**
Gestão centralizada							

do ciclo de vida dos ativos de TI	por máquina	-	14.343	718	-	-	**15.061**
Proteção do correio eletrônico	por usuário	22.826	-	-	-	-	**22.826**
Prevenção de vazamento e uso indevido de informações sensíveis	por máquina	-	14.343	718	-	-	**15.061**

7.3.2. Justificativas da estimativa da demanda:

7.3.2.1. Para as licenças do tipo proteção avançada de endpoints, gestão centralizada do ciclo de vida dos ativos de TI e prevenção de vazamento e uso indevido de informações sensíveis, foi considerado, para fins de estimativa da demanda, o quantitativo atual de máquinas identificado por meio do levantamento do parque computacional.Tal critério reflete de forma fidedigna a base instalada existente, assegurando a aderência da contratação às reais necessidades operacionais, bem como a adequada cobertura de segurança dos ativos em uso, sem superdimensionamento ou subdimensionamento da solução.

7.3.2.2. Com relação a Proteção de servidores físicos, virtuais e ambientes em nuvem, apesar da quantidade levantada ser superior ao estimado, considerou-se a quantidade em uso na console, pois está em andamento a contratação de solução de multinuvem com ênfase em nuvem soberana, a ser implementada e sustentada em ambiente de Data Center da Empresa de Tecnologia e Informações da Previdência - DATAPREV e, ainda, a transferência dos HFRJ para as prefeituras.

7.3.2.3. Referente ao licenciamento para proteção do correio eletrônico, foi considerado para estimativa da demanda o quantitativo de usuários identificado por meio do levantamento do parque computacional.

8. Levantamento de soluções

8.1 Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas:

8.1.1. Considerando tratar-se de levantamento de soluções disponíveis que podem atender à necessidade da contratação, identificou-se as seguintes contratações/aquisições de solução de segurança realizadas por órgãos da Administração Pública:

Órgão	Contrato /Pregão	Objeto	Solução Adotada
Ministério da Cultura	41/2024	Contratação de subscrição de softwares de segurança e antivírus para servidores de rede, storage, microcomputadores, smartphones e tabletes (endpoint protection) com suporte e atualização por 36 (trinta e seis) meses	Solução de antivírus *Kaspersky*
BNDS	22/2025	Contratação de subscrição de uso, atualização e suporte técnico especializado para solução de antivírus Symantec Endpoint Protection para servidores Windows.	Solução de antivírus Symantec Endpoint Protection para servidores Windows.
IBAMA	16/2023	Contratação de solução de tecnologia da informação e comunicação de solução de proteção contra ameaças avançadas (next generation antivírus -	Solução de segurança para proteção de endpoint (NGAV

		ngav) baseada em agente com funcionalidade de edr (“endpoint detection and response”), com suporte, garantia e atualização por 36 meses	– Next Generation endpoint),
SUPERINTENDÊNCIA DO DESENVOLVIMENTO DO NORDESTE	10/2025	Contratação de licenças de uso de antivírus Kaspersky Endpoint Security for Business Select, com atualização contínua por 36 (trinta e seis) meses, para servidores, estações Linux e Windows.	Licenças de uso de antivírus *Kaspersky Endpoint Security for Business Select*
MINISTÉRIO DA AGRICULTURA E PECUÁRIA	28/2023	Contratação de serviços de subscrição de licenças de software relacionados à segurança integrada para estações de trabalho e ambiente corporativo, baseado nas soluções atualmente instaladas no MAPA com foco na monitoração e proteção da segurança tecnológica por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento	Solução de segurança Symantec
EMBRATUR	PE 90006 /2025	Contratação de empresa para fornecimento de solução integrada de segurança da informação com fornecimento de licenças e serviços	Solução de segurança Symantec

8.2. As alternativas do mercado:

8.2.1. Conforme discorrido na Seção 7. Estimativa da Demanda, atualmente, o MS mantém subscrições da solução Symantec, atual Broadcom, como parte de sua estratégia de segurança das informações em atendimento controles previstos no Programa de Privacidade e Segurança da Informação - PPSI 2.0.

8.2.2. Atualmente, existem no mercado diversos fabricantes de soluções de segurança, ofertadas de forma integrada ou composta.

8.2.3. Diante disso, considerando a pesquisa realizado junto a fornecedores, foram apresentadas as seguintes soluções corporativas disponíveis no mercado:

- Symantec Broadcom;
- CB SAFE (CyberBulk Segurança Cibernética);
- Cynet,
- Syxsense;
- Netwrix Endpoint Protector;
- Crowdstkike
- Forcepoint;
- SOPHOS;
- SentinelOne;
- HCLSoftware; e
- Proofpoint.

8.2.4. A Gartner define uma plataforma de proteção de *endpoints* (EPP) como um *software* de segurança projetado para proteger *endpoints* gerenciados - incluindo desktops, laptops, desktops virtuais, dispositivos móveis e, em alguns casos, servidores - contra ataques maliciosos conhecidos e desconhecidos;

8.2.5. O Quadrante Mágico da Gartner (em inglês, *Gartner Magic Quadrant*) é uma metodologia de pesquisa e análise de mercado desenvolvida pela consultoria Gartner Inc., que avalia e posiciona empresas fornecedoras de tecnologia com base em dois eixos principais: capacidade de execução *(ability to execute)* e amplitude de visão *(completeness of vision)*;

8.2.6. Com base nesses critérios, os fornecedores são posicionados em um gráfico dividido em quatro quadrantes: líderes *(leaders)*, desafiadores *(challengers)*, visionários *(visionaries)* e nicho *(niche players)*;

8.2.7. Abaixo, apresentamos o Quadrante Mágico para Plataformas de Proteção de *Endpoints*, com foco nos principais posicionamentos e implicações:

Figure 1: Magic Quadrant for Endpoint Protection Platforms

https://evolutiatec.com.br/insights-do-quadrante-magico-da-gartner-de-2025-para-epp/

8.2.8. Acerca do *Magic Quadrant*, a linha de *Leaders* manteve nomes consolidados, como: *CrowdStrike*, *Microsoft (Defender)*, *SentinelOne*, *Palo Alto Networks*, *Trend Micro* e *Sophos*, refletindo maturidade de produto, amplitude de oferta (EDR + EPP) e capacidade de execução;

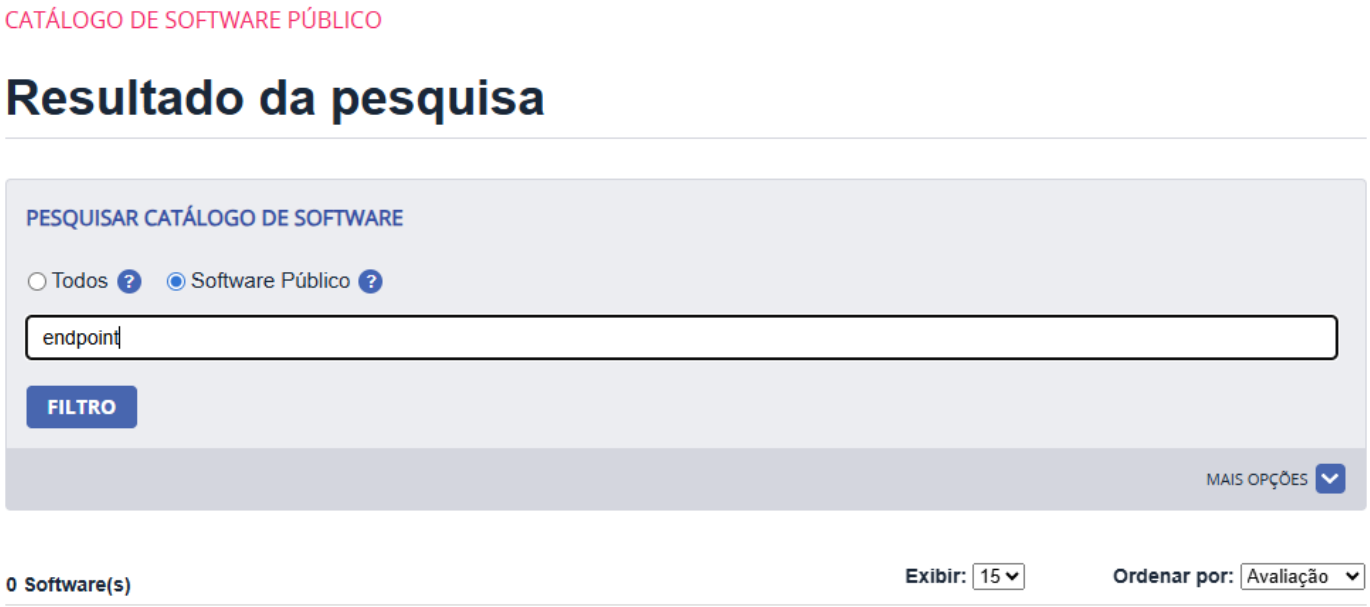
8.2.9. Referente aos *Visionaries* / *Challengers* / *Niche*, observam-se fornecedores como *Bitdefender*, *Check Point*, *Cisco* com abordagens inovadoras ou foco vertical; já *Fortinet*, *WithSecure*, *Cybereason* e *Broadcom* figuram em segmentos de nicho com ofertas mais especializadas;

8.2.10. Torna-se oportuno observar que, para quem está avaliando tecnologia de proteção de *endpoints*, este quadrante pode servir como referência estratégica, mas não como única base de decisão, uma vez ser importante ver os requisitos específicos da organização, integração com outras soluções, custo, suporte local, etc;

8.2.11. A escolha do fornecedor deve considerar não só o posicionamento no relatório, mas também fatores como práticas de implementação, experiência local, alinhamento com a estratégia de segurança da organização e evolução futura (*roadmap* de produtos).

8.3. A existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações;

8.3.1. Em pesquisa realizada no Catálogo de Software Público Brasileiro, disponível em https://softwarepublico.gov.br/social/search/software_infos não foi identificado software que atenda à necessidade objeto desse estudo.



8.3.2. Além disso, foi realizada busca na internet de soluções de software livre (open source) ou gratuitas que, combinada, podem atender, de forma parcial ou complementar, a demanda do MS.

- Para proteção de endpoints e servidores: ClamAV (antivírus open source);
- Detecção e Resposta (SIEM/EDR híbrido): Wazuk plataforma de segurança open source para detecção de intrusões e correlação de eventos;
- Gestão Centralizada de Ativos: GLPI + FusionInventory/OCS Inventory (GLPI é um sistema livre de inventário e gestão de ativos; FusionInventory/OCS faz coleta automática de hardware e software);
- Proteção de correio eletrônico: SpamAssassin (fitro antispam open source) ou Rspamd (sistema moderno de filtragem);
- Prevenção de Vazamento de Dados (DLP): OpenDLP (projeto open source para descoberta de informações sensíveis em endpoints/servidores).

8.4. As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

8.4.1. Os padrões, modelos do ePing, eMag, ICP-Brasil e ePwg foram analisados no contexto da contratação e, considerando que se trata da contratação de subscrições proprietárias, sem desenvolvimento sob demanda, conclui-se que tais referenciais não se aplicam ao presente caso.

8.5. As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

Manutenção da solução atualmente em uso (Symantec/Broadcom)		
Aspecto	**Descrição da Necessidade**	**Grau de Adequação**
Infraestrutura	Não há necessidade de adequação	**-**
Licenciamento	Atualização do quantitativo ou atualizações de versão na console	**Baixo**

Compatibilidade Técnica	Solução compatível com atual ambiente do MS.	**Baixo** Necessidade de verificar novos ativos.
Integração com Sistemas Internos	Nenhuma alteração significativa, visto que as integrações já estão em operação	**Nula**

Substituição da solução atual por uma nova solução corporativa		
Aspecto	**Descrição da Necessidade**	**Grau de Adequação**
Infraestrutura	A depender da solução escolhida, poderá ser necessária a adoção de consoles em nuvem (SaaS) e/ou instalação de componentes locais (gateways, servidores de gerenciamento, appliances virtuais, conectores). Pode demandar adequações de rede, firewall, DNS, proxy, VPN e conectividade com serviços do fabricante.	**Médio** Exige equipe técnica treinada e capacitada para atuar na nova solução
Desinstalação da Solução Anterior	Necessário planejamento para remoção do agente *Symantec (endpoints e servidores)* e desativação gradual dos módulos (DCS, Altiris, SMG, DLP), antes da instalação do novo agente, evitando conflitos.	**Alto** Exige execução coordenada e e controle de risco para evitar janelas sem proteção.
Compatibilidade Técnica	Necessária validação de compatibilidade com sistemas operacionais suportados, ambientes críticos, workloads em nuvem, servidores virtualizados, proxies, VPN, políticas de hardening, além de integrações com SOC. Também deve ser avaliado impacto de desempenho do agente e requisitos mínimos.	**Médio a Alto** Requer testes em ambiente de homologação, mas soluções corporativas costumam ter ampla compatibilidade.
Integração com Sistemas Internos	Necessária integração com diretórios (AD), ferramentas de inventário, ITSM, SIEM, SOC, e eventualmente com soluções de e-mail (Exchange/M365) e gateways. Em geral, fabricantes corporativos fornecem APIs, conectores e integrações prontas.	**Médio** Integrações normalmente são viáveis com conectores do fabricante, mas exigem configuração e validação.
Migração de Políticas de Segurança	Necessária revisão e migração das políticas existentes (perfis de proteção, exceções, regras, quarentena, controle de aplicações, isolamento, alertas, regras de e-mail e políticas de DLP). A migração tende a ser parcialmente manual, pois os modelos entre fabricantes diferem.	**Alto** Exige reconstrução parcial /total das políticas e validação rigorosa para evitar lacunas de proteção.

Adoção de solução open source ou gratuitas		
Aspecto	**Descrição da Necessidade**	**Grau de Adequação**
Infraestrutura	Necessária implantação e sustentação de infraestrutura própria para múltiplos componentes (ex.: servidores para Wazuh /Elastic, GLPI, banco de dados, mail gateway antispam /antimalware, repositórios, storage para logs e retenção). Exige planejamento de alta disponibilidade, backup, hardening, atualização contínua e monitoramento.	**Alto** Exige infraestrutura robusta e equipe especializada para operação contínua.
	Necessário planejamento para remoção coordenada dos agentes e componentes Symantec/Broadcom (endpoints,	**Médio a Alto**

Desinstalação da Solução Anterior	servidores, DLP, gateways), evitando conflitos com novos agentes (Wazuh, inventário) e garantindo continuidade mínima de proteção durante a transição.	Exige execução coordenada, com janelas de mudança e gestão de riscos.
Compatibilidade Técnica	Necessária avaliação detalhada de compatibilidade com Windows, Linux e macOS, ambientes restritos, proxy/VPN, requisitos de kernel/driver, performance e conflitos com softwares existentes. Além disso, deve-se validar a cobertura funcional.	**Alto** Requer testes extensivos e validação funcional, pois não há equivalência direta em várias capacidades.
Integração com Sistemas Internos	Exigida integração por APIs e conectores com AD/Azure AD (quando aplicável), SIEM/SOC, ITSM, inventário, sistemas de autenticação e fluxos de incidentes. Em software livre, a integração costuma ser manual, com maior esforço de customização e manutenção.	**Alto** Integrações dependem de desenvolvimento /configuração interna e manutenção contínua.
Migração de Políticas de Segurança	Necessária reengenharia completa das políticas atuais (antimalware, firewall, regras, exceções, quarentena, alertas, DLP, e-mail, inventário e conformidade). Em geral não há importação automática entre Symantec e ferramentas livres; as políticas precisam ser reconstruídas e ajustadas por tentativa, erro e validação.	**Muito Alto** Exige reconstrução integral das políticas, com alto risco operacional e de lacunas de segurança.

8.6. Os diferentes modelos de prestação do serviço;

8.6.1. No contexto de contratação de solução de segurança para endpoints, servidores, e-mail, gestão de ativos e DLP, os principais modelos de prestação de serviços disponíveis no mercado são:

a) On-premises;

b) SaaS (*Software* como Serviço);

c) Modelo Híbrido (*on-premises* + *cloud*); ou

d) Serviço Gerenciado (MSSP - *Managed Security Service Provider*).

8.6.1.1. **No modelo SaaS (Software as a Service)** - a solução é disponibilizada como serviço em nuvem, hospedada e operada pelo fabricante. A contratante instala apenas agentes ou conectores locais. É o modelo predominante no mercado atual de EDR/XDR e segurança corporativa. Principais características:

- Console de gestão hospedado em nuvem;
- Atualizações automáticas, assinaturas e funcionalidades;
- Alta escalabilidade;
- Arquitetura multi-tenant;
- Conectividade segura via HTTPS/TLS;
- Backup e alta disponibilidade geridos pelo fornecedor.

8.6.1.2. **No modelo On-Premises** - a solução é instalada integralmente no data center do órgão, incluindo console, banco de dados e servidores de gerenciamento. Modelo ainda utilizado em órgãos públicos, mas com tendência de migração para híbrido ou SaaS. Principais características:

- Controle total sobre infraestrutura;
- Necessidade de servidores físicos/virtuais dedicados;
- Atualizações manuais ou programadas;
- Necessidade de backup, redundância e hardening local.

8.6.1.3. **No modelo Híbrido** a solução é a combinação de componentes SaaS e on-premises. Exemplo: console de endpoint em nuvem, DLP ou gateway de e-mail local e Conectores on-prem para integração com AD. Modelo muito utilizado em órgãos públicos federais. Principais características:

- Integração entre ambientes via APIs;
- Necessidade de conectores locais;
- Arquitetura parcialmente descentralizada.

8.6.1.4. **No modelo Perpétuo** - se trata da aquisição definitiva da licença do software, com pagamento separado de manutenção. Modelo em declínio no segmento de cibersegurança. Principais características:

- Instalação local;
- Direito de uso permanente da versão adquirida;
- Atualizações dependem de contrato de manutenção.

8.7. Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

8.7.1. No mercado de segurança da informação, as soluções voltadas à proteção de endpoints, servidores, correio eletrônico, gestão de ativos e prevenção de vazamento de dados podem ser estruturadas de diferentes formas, variando quanto à especificação técnica, composição e características dos bens e serviços associados.

a) Solução integrada de um único fabricante - Consiste na contratação de uma plataforma de segurança composta por múltiplos módulos do mesmo fabricante, com gestão centralizada e integração nativa entre componentes. Esse modelo tende a reduzir riscos de incompatibilidade, facilitar a operação, consolidar logs e políticas, e simplificar o suporte técnico, uma vez que a responsabilidade de integração e interoperabilidade recai sobre um único fornecedor.

b) Solução composta por vários fabricantes: Nesse modelo, cada componente é adquirido de um fabricante especializado, buscando-se maximizar a profundidade técnica de cada domínio. A integração é realizada por meio de APIs, conectores e/ou correlação em SIEM/SOAR.

Embora possa trazer ganhos técnicos em funcionalidades específicas, esse modelo aumenta a complexidade operacional, exige maior maturidade de governança e pode ampliar riscos relacionados à interoperabilidade, à responsabilização em incidentes e ao custo total de operação.

8.8. A possibilidade de aquisição na forma de bens ou contratação como serviço;

8.8.1. De acordo com o item acima, verifica-se que a maioria dos fabricantes disponibiliza a solução de segurança na forma de serviços, dessa forma, será mantido o modelo de contratação por meio de prestação de serviço.

8.9. A ampliação ou substituição da solução implantada;

8.9.1. Caso seja mantida a solução atualmente em uso no MS, alguns itens sofreram redução do quantitativo, considerando o levantamento atualizado do parque computacional.

8.9.2. Ademais, caso seja considerado viável, poderá ser realizada a substituição da solução implantada por de outro fabricante ou a adoção de software livre.

8.10. As diferentes métricas de prestação do serviço e de pagamento;

Forma de Pagamento	Descrição	Periodicidade
Por licença/assinatura ativa	Pagamento proporcional à quantidade de dispositivos cobertos.	Anual
Por nível de suporte contratado	Pagamento vinculado ao tipo de suporte (básico, avançado, 24x7).	Anual
Por indicadores de desempenho (SLA)	Penalidades em caso de indisponibilidade ou descumprimento de prazos.	Avaliação Mensal

8.10.1. Com base no levantamento de soluções realizado, foram identificados três cenários possíveis para o atendimento da necessidade, a saber:

ID	Descrição da solução (ou cenário)
1	Manutenção da solução atualmente em uso (Symantec/Broadcom)

2	Substituição da solução atual por uma nova solução corporativa
3	Adoção de solução de software livre

9. Análise comparativa de soluções

9.1. Análise dos Cenários

9.1.1. Cenário 1 - Manutenção da solução atualmente em uso (Symantec/Broadcom):

9.1.1.1. Neste cenário, considera-se a continuidade da solução atualmente em uso no Ministério da Saúde, composta por subscrições Symantec/Broadcom que abrangem proteção avançada de *endpoints*, proteção de servidores, proteção do correio eletrônico, prevenção de vazamento e uso indevido de informações sensíveis e gestão centralizada do ciclo de vida dos ativos de TI;

9.1.1.2. A solução de segurança Broadcom (Symantec) está implementada no Ministério da Saúde há mais de uma década, consolidando-se como o alicerce da defesa cibernética do órgão. Esse longo período de operação permitiu atingir o nível máximo de maturidade técnica. O corpo técnico detém o domínio pleno da arquitetura, o que possibilita uma administração de alta performance e respostas imediatas.

9.1.1.3. O Ministério da Saúde utiliza o modelo de licenciamento mais abrangente do fabricante, permitindo o uso integrado de diversos módulos de segurança. Esta suíte provê proteção em arquitetura híbrida, abrangendo nativamente o ambiente on-premise e infraestruturas em nuvem (cloud), já operando com gerenciamento em console de nuvem e suporte nativo a ambientes multicloud. Esta infraestrutura atual dispensa novos investimentos em hardware ou software de gestão.

9.1.1.4. A seguir, apresenta-se os pricipais benefícios para manutenção do referido cenário:

Integração Sistêmica com o Security Operations Center - SOC (Securonix):

A resiliência cibernética do órgão é sustentada pela integração profunda de toda a suíte **Broadcom (Endpoint EDR, Anti-Spam e Servidores) com o SIEM (Securonix) do SOC.** A telemetria enviada ao SOC é holística e correlacionada. A troca da solução invalidaria os playbooks de resposta automatizada e as regras de detecção validadas ao longo de anos, reduzindo drasticamente a eficácia da defesa durante a migração.

Base de Conhecimento e Preservação de Dados Históricos:

A permanência da solução preserva uma extensa Base de Conhecimento técnica construída ao longo de mais de uma década. Este repositório contém o registro detalhado de comportamentos específicos do ambiente do MS, soluções de contorno para sistemas legados e padrões de ameaças identificados no domínio @saude.gov.br. A descontinuidade resultaria na perda deste histórico consultivo, elevando o Tempo Médio de Atendimento (MTTR).

Governança Centralizada e Capilaridade via Altiris:

Dada a vasta capilaridade das unidades do Sistema Único de Saúde (SUS), a utilização do Altiris (Symantec Endpoint Management) é vital. O Altiris possibilita o gerenciamento centralizado **de 15.061 ativos (estações de trabalho e servidores)**, provendo visibilidade em tempo real. Sem esta integração, a manutenção da conformidade (patches e inventário) em unidades remotas seria severamente comprometida.

Maturidade em Prevenção de Perda de Dados do Data Loss Prevention (DLP):

A implementação do DLP atingiu um estágio de refinamento técnico que assegura a proteção de dados sensíveis em conformidade com a LGPD. A solução atua de forma integrada na rede local e no ambiente Microsoft Cloud. O ajuste fino das regras foi construído sob medida para o fluxo do Ministério, garantindo conformidade sem impactar a produtividade.

Eficiência em Proteção de Mensageria (Anti-Spam):

A solução de anti-spam atua como a barreira primária contra phishing e ransomware. A eficiência atual é fruto de anos de calibração para o tráfego do órgão, minimizando falsos positivos em comunicações institucionais críticas e garantindo que o fluxo de e-mails do MS não sofra interrupções indevidas.

9.1.1.5. O foco principal deste cenário é preservar o ambiente atual, garantindo continuidade operacional, previsibilidade de custos e evitando riscos associados a uma migração tecnológica complexa. Com isso, manter a atual solução apresenta os seguintes aspectos técnicos e operacionais:

Aspectos Técnicos e Operacionais	Análise
Arquitetura e Compatibilidade	Total compatibilidade com o ambiente existente, não requer migração, nem reinstalação em massa de agentes.
Segurança e Desempenho	Solução madura, com recursos de EDR *(Endpoint Detection and Response)*, prevenção contra *malware*, *ransomware* e controle de dispositivos. A eficácia depende da atualização das assinaturas e políticas.
Integração	Já integrada a sistemas de inventário e gestão de ativos, além de integração nativa com AD e SIEMs.
Suporte Técnico e Continuidade Operacional	Suporte consolidado, com equipe interna já treinada no uso do console. Menor curva de aprendizado e riscos de indisponibilidade.
Custo e Investimento	Custo restrito à renovação de licenças e suporte; evita despesas de migração, novos treinamentos e reinstalações.
Governança e Gestão de Riscos	Mantém rastreabilidade e conformidade das políticas vigentes. Risco baixo de transição e impacto operacional mínimo.

9.3.1.6. Complementar aos aspectos técnicos e operacionais, registra-se na tabela a seguir os aspectos estratégicos:

Aspectos Estratégicos	Análise
Custo e Licenciamento	Manter a solução atual evita custos imediatos de migração e treinamento.
Risco Operacional	O cenário é de baixo risco técnico, pois mantém infraestrutura validada e compatível.
Aderência a requisitos de segurança governamental	A solução mantém conformidade com padrões de segurança corporativa e *compliance*, atendendo requisitos de auditoria e rastreabilidade.
Dependência de Fornecedor	O ambiente permanece fortemente vinculado ao ecossistema Broadcom, reduzindo flexibilidade para integrações futuras ou adoção gradual de componentes de terceiros.

9.3.1.7. Para mais, exploram-se as vantagens e desvantagens do **Cenário 1** na tabela a seguir:

Vantagens	Desvantagens
Continuidade operacional sem impacto nos usuários finais;	Pode limitar ganhos de inovação e integração com novas tecnologias de *threat hunting* e IA;
Zero impacto na operação atual;	Dependência do fornecedor atual (*lock-in* tecnológico);
Custos previsíveis e menor risco de falhas;	Eventual defasagem tecnológica frente às soluções líderes em IA comportamental e resposta automatizada.
Aproveitamento de conhecimento técnico já existente.	

9.3.1.8. Esse cenário apresenta como principais vantagens a preservação da arquitetura de segurança existente, a redução de riscos operacionais, a compatibilidade com os sistemas e processos já consolidados e o aproveitamento do conhecimento técnico da equipe interna;

9.3.1.9. A manutenção da solução Symantec/Broadcom é uma opção conservadora e de baixo risco operacional, indicada para contextos em que estabilidade, *compliance* e continuidade são prioritários.

9.3.1.10. Diante do exposto, **o cenário 1 - Manutenção da solução atualmente em uso (Symantec/Broadcom) apresenta-se como alternativa tecnicamente viável.**

9.3.2. Cenário 2 - Substituição da solução atual por uma nova solução corporativa:

9.3.2.1. Neste cenário, considera-se a substituição integral da solução atual por uma nova suíte coporativa de segurança de outro fabricante, com características técnicas equivalentes e capazes de atender às mesmas funções: proteção de *endpoints*, servidores, e-mail corporativo, dados e gestão de ativos.

9.3.2.2. Conforme demostrado no levantamento de soluções, existem no mercado diversos fabricantes aptosa atender à necessidade do MS.

9.3.2.3. Este cenário envolve a substituição dos agentes instalados, a integração de um novo console de gerenciamento e a implatação e migraçã das políticas de segurança.

9.3.2.4. Dito isto, exploram-se os seguintes aspectos técnicos e operacionais:

Dimensão	Análise
Arquitetura e Compatibilidade	Exige a migração de agentes e reconfiguração completa de políticas e conectores e dependendo da solução.
Segurança e Desempenho	Soluções líderes no Gartner (ex.: *CrowdStrike*, *Defender*, *SentinelOne*) oferecem detecção baseada em IA, resposta automatizada e visibilidade em tempo real, com eficácia superior em ameaças modernas.
Integração	Pode demandar novos conectores com AD e plataformas SOC. Algumas soluções têm API's abertas e integração nativa com Microsoft 365, Azure ou GCP.
Suporte Técnico e Continuidade Operacional	Necessita de treinamento da equipe técnica do MS e período de transição entre as soluções, podendo haver sobreposição de agentes temporária e riscos de incompatibilidade.
Custo e Investimento	Envolve custos de aquisição de novas licenças, migração, treinamento e eventuais consultorias de implantação.
Governança e Gestão de Riscos	Melhora visibilidade e governança de incidentes; pode simplificar conformidade com LGPD e políticas internas de segurança. Requer atualização de normativos e documentação técnica.

9.3.2.5. Como já mencionado neste Estudo, o MS utiliza a plataforma Symantec/Broadcom Endpoint Protection, uma solução consolidada, com arquitetura híbrida (*on-premise* e nuvem), que provê antivírus, *firewall*, controle de dispositivos e prevenção de intrusões. No entanto, o avanço das ameaças modernas (*ransomware*, ataques *fileless*, movimentos laterais e *phishing* avançado) e a tendência de adoção de EDR/XDR e inteligência em nuvem, torna necessária a avaliação de alternativas tecnológicas mais integradas e preditivas;

9.3.2.6. Entretanto, torna-se relevante pontuar que a migração de uma solução de proteção de *endpoints* representa uma operação crítica dentro da infraestrutura de segurança de qualquer órgão público, especialmente em um ambiente com a complexidade e a capilaridade do Ministério da Saúde. Esse processo impacta diretamente a disponibilidade, a integridade e a continuidade dos serviços digitais, demandando planejamento técnico rigoroso, mitigação de riscos e governança contínua;

9.3.2.7. A migração, portanto, deve ser encarada não apenas como troca de ferramenta, mas como um reposicionamento da arquitetura de defesa, alinhando-se às melhores práticas de *Zero Trust*, resposta automatizada e telemetria unificada. Isto posto, a substituição da solução de *endpoint* envolve uma série de componentes técnicos que precisam ser avaliados cuidadosamente, como:

a) Compatibilidade e inventário, visto que antes de iniciar qualquer migração, é fundamental realizar um inventário detalhado de:

- Sistemas operacionais em uso;
- Aplicações corporativas críticas que interagem com os agentes de segurança; e
- Perfis de usuário e políticas de grupo (GPOs).

b) Remoção do agente atual, uma vez que o agente da *Symantec* atua em nível profundo do sistema e a sua remoção inadequada pode gerar conflitos, falhas de comunicação ou desativação temporária de proteção, o que torna recomendável os seguintes fatores:

- Utilizar ferramentas de desinstalação automatizada;
- Adotar políticas de coexistência temporária; e
- Garantir que não haja sobreposição de *drivers* entre o agente antigo e o novo.

c) Instalação e configuração do novo agente:

- Via SCCM / *Intune* (Microsoft) ou *Scripts* de implantação com validação automática;
- Os consoles de gestão devem ser previamente configurados com: políticas de detecção, quarentena e resposta; integração com o *Active Directory*, SIEM, SOAR e sistemas de inventário; e perfis de alertas e *dashboards* personalizados para as equipes do MS.

9.3.2.8. Adstrito a isto, durante a migração, o órgão enfrentará uma janela crítica em que parte dos *endpoints* poderá estar temporariamente desprotegida. De modo que será necessário avalidar as seguintes adoções:

a) Implantação em ondas (*waves*) - por unidade, região ou tipo de usuário;

b) Monitoramento em tempo real;

c) Coexistência temporária de agentes em máquinas piloto;

d) *Backups* de políticas e *logs* da solução antiga, para auditoria e rastreabilidade; e

e) Garantir a rastreabilidade dos eventos, mesmo durante a transição, para que não haja perda de visibilidade sobre incidentes em andamento.

9.3.2.9. Abaixo apresenta-se um quadro comparativo técnico das soluções de proteção de *endpoint* identificadas na pesquisa de mercado, voltado à análise de uma possível substituição da plataforma atual do Ministério da Saúde:

Fabricante / Solução	Modelo de Implantação	Principais Capacidades	Integração e Operação	Complexidade de Migração	Requisitos Técnicos	Avaliação Técnica Geral
Symantec (Broadcom)	SaaS, On-premises e híbrido	Endpoint, EDR, DLP, Email Security, Data Center Security	Integração consolidada com AD, SIEM e ITSM	Baixa (manutenção)	Infraestrutura já implantada	Alta aderência e menor risco operacional
CB SAFE	SaaS	EDR, antivírus, gestão centralizada	Integração via APIs	Média	Dependência de conectividade cloud	Adequada para ambientes médios
Cynet	SaaS (cloud-native)	XDR, EDR, resposta automatizada	Integração simplificada	Média	Consoles em nuvem	Boa consolidação tecnológica
Syxsense	SaaS	EDR + Patch Management + inventário	Integração com AD	Média	Agentes atualizados	Indicada quando há foco em gestão integrada
Netwrix Endpoint Protector	SaaS ou On-prem	DLP para endpoints e dispositivos	Integração com diretórios e SIEM	Média	Servidor dedicado (on-prem)	Solução complementar focada em DLP
CrowdStrike	SaaS (cloud-native)	EDR/XDR avançado, threat intelligence	Alta integração via API	Média	Conectividade contínua	Elevada maturidade tecnológica

Forcepoint	SaaS ou híbrido	DLP corporativo, CASB, Web Security	Integração robusta	Média a Alta	Infraestrutura estruturada	Forte aderência para DLP estratégico
Sophos	SaaS ou On-prem	Endpoint, XDR, Firewall integrado	Integração nativa com firewall	Média	Consolidação de ambiente pode ser necessária	Boa opção para ambientes integrados
SentinelOne	SaaS	EDR/XDR com IA, rollback ransomware	APIs abertas	Média	Arquitetura cloud-first	Alto nível tecnológico
HCLSoftware	On-prem ou híbrido	Gestão de endpoints (BigFix), patch e segurança	Integração corporativa ampla	Média a Alta	Infraestrutura dedicada	Indicado para grandes ambientes
Proofpoint	SaaS	Email Security, DLP, anti-phishing	Integração com M365 e SIEM	Baixa a Média	Integração com correio eletrônico	Excelente solução para e-mail corporativo

9.3.2.10. Neste contexto, demonstra-se as seguintes vantagens e desvantagens para o **Cenário 2**:

Vantagens	Desvantagens
Modernização da arquitetura de segurança, com IA e EDR nativos;	Risco operacional durante a migração (interrupções, duplicidade de agentes);
Potencial redução de vulnerabilidades e incidentes não detectados;	Curva de aprendizado e necessidade de treinamento técnico;
Melhoria na integração com plataformas de nuvem e resposta automatizada;	Maior custo inicial e necessidade de nova homologação e testes de compatibilidade;
Ganho em desempenho e centralização via nuvem.	Dependência de conectividade e SLAs de serviço em soluções 100% SaaS;
	Infraestrutura de rede: aumento de tráfego para nuvem (telemetria e atualizações de assinatura);
	Políticas de segurança: revisão das exclusões, exceções e regras de bloqueio conforme comportamento da nova solução;
	Integração com processos ITSM: adequação dos fluxos de atendimento e resposta a incidentes.

9.3.2.11. Resta consolidado que este cenário demandaria a execução de serviços adicionais, como implantação, migração, integração e treinamento, a fim de garantir a continuidade da proteção durante o período de transição;

9.3.2.12. Diante do exposto, **o cenário 2 - Substituição da solução atual por uma nova solução corporativa, apesar dos riscos associados, apresenta-se como alternativa tecnicamente viável.**

9.3.3. Cenário 3 - Adoção de solução de *software* livre:

9.3.3.1. Neste cenário será implantada uma solução de segurança e proteção de *endpoints* baseada em *software* livre ou soluções integradas mantidas por comunidades de desenvolvimento, fundações ou consórcios tecnológicos, conforme identificado no levantamento de soluções.

9.3.3.2. Tais soluções, normalmente, oferecem componentes de antivírus, monitoramento de integridade, detecção e resposta a incidentes (EDR) e integração com SIEMs.

9.3.3.3. As soluções *open source* oferecem recursos relevantes, tais como:

a) Monitoramento de integridade de arquivos *(FIM - File Integrity Monitoring)*;

b) Coleta e correlação de *logs* de eventos de segurança;

c) Análise comportamental básica e alertas de incidentes;

d) Integração com sistemas SIEM e *dashboards* via *Kibana* ou *Grafana*; e

e) Possibilidade de integração com antivírus *open source* (como *ClamAV*).

9.3.3.4. Porém, existem limitações técnicas em relação a soluções comerciais líderes de mercado, como menor capacidade de resposta automática a ameaças *(automated remediation)*, ausência de inteligência de ameaças *(Threat Intelligence)* nativa e em tempo real, menor cobertura de *endpoints* móveis e ambientes híbridos *(Windows/Linux)* e dependência de configuração e *tunning* manual para otimizar detecção e reduzir falsos positivos;

9.3.3.5. Em que pese as soluções *open source* cumprirem em parte dos requisitos de proteção, elas não atingem o mesmo nível de eficácia, automação e integração oferecido por soluções comerciais EDR/XDR consolidadas. A partir disso, demonstra-se na tabela a seguir os riscos identificados:

Tipo	Descrição	Impacto
Técnico	Falhas de detecção avançada (sem IA/ML nativos).	Alto
Operacional	Sobrecarga da equipe técnica e curva de aprendizado elevada.	Médio
Governança	Falta de SLA e garantia formal de atualização.	Alto
Segurança	Possível atraso em *patches* críticos se a comunidade for lenta.	Médio
Continuidade	Dependência de comunidade sem compromisso de longo prazo.	Médio

9.3.3.6. Neste contexto, demonstra-se as seguintes vantagens e desvantagens para o **Cenário 3**:

Vantagens	Desvantagens
Eliminação de custos de licenciamento;	Necessidade de maior capacidade técnica interna para gestão;
Ausência de dependência de fornecedores comerciais *(vendor lock-in)*;	Ausência de garantias formais de suporte e SLA;
Possibilidade de auditoria do código-fonte;	Menor integração com plataformas corporativas e de nuvem proprietárias;
Possível flexibilidade para customizações específicas.	Eventual limitação em recursos avançados de EDR/XDR baseados em IA e automação;
	Maior esforço de integração e manutenção, exigindo equipe especializada.

9.3.3.7. O cenário de *software* livre geralmente é considerado tecnicamente viável em ambientes com equipe de segurança madura e infraestrutura própria de monitoramento (SOC), mas economicamente e operacionalmente inviável em órgãos que dependem de suporte contínuo, integração com ecossistemas corporativos e garantias contratuais, como é o caso do Ministério da Saúde;

9.3.3.8. Assim, **a escolha pelo cenário 3 - Adoção de solução de software livre, torna-se uma alternativa tecnicamente inviável.**

9.4. Conclusão

9.4.1. Apresenta-se o seguinte resumo dos cenários analisados anteriormente:

Critério	Cenário 1	Cenário 2	Cenário 3
Custo inicial	Baixo	Médio/Alto	Baixo
Custo operacional	Baixo	Variável (*SaaS* pode reduzir infraestrutura)	Alto
Inovação tecnológica	Médio	Alto	Médio
Risco de implantação	Baixo	Moderado/Alto	Moderado/Alto
Desempenho e eficácia	Alto	Alto	Baixo
Curva de aprendizado	Nenhuma	Alto	Alto
Dependência de fornecedor	Alto	Alto	Baixo
Governança e auditoria	Consolidada	Exigirá readequação	Exigirá readequação

9.5. Análise comparativa dos cenários

9.4.1. Análise comparativa das soluções propostas sob os **aspectos qualitativos**:

Necessidades		**Manutenção da solução atualmente em uso (Symantec/Broadcom)**	**Substituição da solução atual por uma nova solução corporativa**	**Adoção de solução de software livre**
	Garantir a proteção de estações de trabalho, notebooks e servidores, contra vírus, malwares, ransomware e outras ameaças cibernéticas;	Atende	Atende	Atende parcialmente ou depende de composição
	Assegurar a proteção do correio eletrônico institucional, com recursos de filtragem antispam e antiphishing e antimalware evitando golpes e contaminações via e-mail;	Atende	Atende	Atende parcialmente ou depende de composição
	Prevenir o vazamento de informações sigilosas e dados pessoais sensíveis, em conformidade com a LGPD, por meio de mecanismos de monitoramento e bloqueio de tentativas não autorizadas;	Atende	Atende	Atende parcialmente ou depende de composição

	Oferecer gestão centralizada e visibilidade completa sobre o estado de segurança de todos os ativos do parque tecnológico (estações, servidores, dispositivos móveis e ambientes em nuvem);	Atende	Atende	Atende parcialmente ou depende de composição
	Disponibilizar recursos de resposta e investigação de incidentes, que permitam identificar, conter e remediar ameaças de forma ágil e eficiente;	Atende	Atende	Atende parcialmente ou depende de composição
	Assegurar proteção também em ambientes híbridos, contemplando infraestrutura local (on-premises), nuvem pública e modelos de trabalho remoto;	Atende	Atende	Atende parcialmente ou depende de composição
Negócio	Garantir escalabilidade da solução, de modo a suportar a evolução e o crescimento do parque tecnológico do Ministério da Saúde;	Atende	Atende	Atende parcialmente ou depende de composição

	Disponibilizar relatórios e indicadores de segurança, que apoiem a tomada de decisão, a gestão de riscos e a prestação de contas à alta administração;	Atende	Atende	Atende parcialmente ou depende de composição
	Atender às normas, políticas e legislações vigentes, em especial a LGPD, ao Programa de Privacidade e Segurança da Informação - PPSI 2.0, à Política de Gestão de Riscos do Ministério da Saúde, à Política de Segurança da Informação do MS e às diretrizes do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC);	Atende	Atende	Atende parcialmente ou depende de composição
	Possibilitar suporte técnico contínuo e atualização de assinaturas e bases de proteção, assegurando que a solução se mantenha eficaz contra novas ameaças;	Atende	Atende	Atende parcialmente ou depende de composição

	Garantir a padronização em todos os dispositivos corporativos por meio da gestão centralizada;	Atende	Atende	Atende parcialmente ou depende de composição
	A solução deverá ser composta por módulos integrados, reduzindo o risco decorrente de soluções fragmentadas ou não integradas;	Atende	Atende	Atende parcialmente ou depende de composição
	Prevenir, detectar e responder a ameaças cibernéticas, incluindo malwares, ransomwares, spywares, exploits, ataques de dia zero e ameaças persistentes avançadas;	Atende	Atende	Atende parcialmente ou depende de composição
	Utilizar mecanismos modernos de detecção, como análise comportamental, heurística, aprendizado de máquina e inteligência artificial;	Atende	Atende	Atende parcialmente ou depende de composição
	Permitir resposta automatizada a incidentes, incluindo	Atende	Atende	Atende parcialmente ou depende de composição

	isolamento do endpoint, bloqueio de processos maliciosos e mitigação de danos;			
	Proteger contra ataques baseados em memória e exploração de vulnerabilidades;	Atende	Atende	Atende parcialmente ou depende de composição
	Operar de forma contínua, mesmo em situações de conectividade limitada;	Atende	Atende	Atende parcialmente ou depende de composição
	Ser compatível com os sistemas operacionais utilizados no ambiente institucional;	Atende	Atende	Atende parcialmente ou depende de composição
	Possuir proteção para servidores físicos e virtuais, bem como workloads executados em ambientes de nuvem pública, privada ou híbrida;	Atende	Atende	Atende parcialmente ou depende de composição
	Mecanismos de proteção antimalware e anti-exploit adequados a ambientes de missão crítica;	Atende	Atende	Atende parcialmente ou depende de composição
	Detecção de comportamentos anômalos e tentativas de escalonamento indevido de privilégios;	Atende	Atende	Atende parcialmente ou depende de composição

Tecnológicas				
	Visibilidade centralizada do estado de segurança dos servidores, com alertas e registros de eventos;	Atende	Atende	Atende parcialmente ou depende de composição
	Inventário automatizado de hardware e software;	Atende	Atende	Atende parcialmente ou depende de composição
	Monitoramento do estado de conformidade e segurança dos ativos;	Atende	Atende	Atende parcialmente ou depende de composição
	Distribuição, atualização e gerenciamento remoto dos agentes e políticas de segurança;	Atende	Atende	Atende parcialmente ou depende de composição
	Mecanismos de antispam, antiphishing, antimalware e antifraude;	Atende	Atende	Atende parcialmente ou depende de composição
	Aplicação de políticas de segurança em ambientes locais, em nuvem ou híbridos;	Atende	Atende	Atende parcialmente ou depende de composição
	Geração de relatórios técnicos e gerenciais que subsidiem a tomada de decisão;	Atende	Atende	Atende parcialmente ou depende de composição
	Identificar, classificar e proteger informações sensíveis, pessoais ou estratégicas;	Atende	Atende	Atende parcialmente ou depende de composição

	Monitorar e controlar a movimentação de dados em endpoints, servidores, correio eletrônico e outras canais;	Atende	Atende	Atende parcialmente ou depende de composição
	Gerar registros, alertas e evidências para fins de auditoria e apuração;	Atende	Atende	Atende parcialmente ou depende de composição
	Apoiar a conformidade com legislações e normativos aplicáveis, como a Lei Geral de Proteção de Dados Pessoais (LGPD);	Atende	Atende	Atende parcialmente ou depende de composição
	Correlação de eventos e resposta coordenada a incidentes de segurança;	Atende	Atende	Atende parcialmente ou depende de composição
	Contar com suporte técnico especializado e atualizações contínuas;	Atende	Atende	Atende parcialmente ou depende de composição
	Estar aderente as boas práticas, normas e padrões de segurança da informação.	Atende	Atende	Atende parcialmente ou depende de composição
Resultado		**Atende**	**Atende**	**Não atende**

10. Registro de soluções consideradas inviáveis

10.1. Conforme § 1º do art. 11 da IN SGD 94/2022, após o levantamento das possíveis soluções para a execução dos serviços de Tecnologia da Informação e Comunicação, a equipe de planejamento da contratação concluiu que o cenário abaixo é inviável, conforme justificativas apresentadas na escolha da solução, dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

ID	Descrição da solução (ou cenário)
3	Adoção de solução de software livre.

10.2. A adoção de software livre não se mostra adequada para atendimento integral e seguro das necessidades institucionais, salvo mediante projeto estruturante específico e ampliação significativa da capacidade técnica interna.

11. Análise comparativa de custos (TCO)

11.1. Custos Totais de Propriedade

11.1.1. O *Total Cost of Ownershsip - TCO* ou custo total de propriedade é um método utilizado para calcular o custo global de um produto ou serviço ao longo de seu ciclo de vida, considerando custos diretos e indiretos;

11.1.2. Utiliza-se esse conceito para se referir à estimativa dos custos dos cenários projetados ao longo do uso da solução, possibilitando uma análise mais precisa e abrangente economicamente. Por conseguinte, é necessário estimar os custos de bens e serviços para cada cenário viável;

11.1.3. Registra-se ainda, o que preconiza a Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, a qual orienta que deve ser avaliada a relação custo-benefício de manter a solução implantada ou de substituí-la em casos que, mesmo havendo alto impacto na migração da solução, haja ganhos financeiros para o órgão ou entidade e informa que essa avaliação deve ser executada por meio da análise de TCO dos possíveis cenários, observando as orientações publicadas pela SGD;

11.1.4. Baseando-se nas soluções viáveis, detalhadas na Seção 9 deste Estudo Técnico, quais sejam:

ID	Descrição da solução (ou cenário)
1	Manutenção da solução atualmente em uso (Symantec/Broadcom)
2	Substituição da solução atual por uma nova solução corporativa

11.2. Análise dos Custos Totais de Propriedade

11.2.1. A fim de verificar os custos para manter a solução implantada ou de substituí-la, foi encaminhado Caderno de Cotação (SEI nº 0052279510) a potenciais fornecedores de solução de segurança para proteção de endpoints em estações de trabalho, notebooks e servidores no dia 06/01/2026, com o seguinte escopo:

- A empresa deveria apresentar proposta de preços para os períodos iniciais de 12 (doze) e 36 (trinta e seis) meses para os seguintes cenários:

- **Manutenção da atual solução da fabricante Symantec Broadcom:**

Item	Descrição do item	Part number	Unidade de medida	Quantidade Estimada
1	Subscrição Symantec Endpoint Security Complete	SESC-SES-CLD-SUB	Unidade	15.061
2	Subscrição Symantec Data Center Security	DCS-SRVA-SUB	Unidade	353

3	Subscrição Symantec It Management Suíte (Symantec Altiris)	ALT-SUB	Unidade	15.061
4	Subscrição Symantec Messaging Gateway Hybrid	SMG-HYB-SUB	Unidade	22.826
5	Subscrição Symantec Data Loss Prevention	DLP-ES-SUB	Unidade	15.061

- **Substituição da atual solução**

Item	Descrição do item	Fabricante	Part number /SKU	Unidade de medida	Quantidade Estimada
1	Proteção avançada de endpoints				15.061
2	Proteção de servidores físicos, virtuais e ambientes em nuvem				353
3	Gestão centralizada do ciclo de vida dos ativos de TI				15.061
4	Proteção do correio eletrônico				22.826
5	Prevenção de vazamento e uso indevido de informações sensíveis				15.061
6	**Outros serviços, se houver**				

- Para o cenário de substituição, a solução poderia ser composta por um ou mais fabricantes, desde que apresente-se integração entre seus componentes, garantindo gestão centralizada e operação unificada, sem gerar riscos à segurança da informação.
- Deveria ser informado, ainda, o modelo de disponibilização do software, indicando se ocorreria por meio de: cessão temporária de direitos de uso, licenciamento permanente de direitos de uso, subscrição ou utilização como serviço (Software como Serviço).

11.3. Mapa Comparativo dos Cálculos Totais de Propriedade (TCO)

11.3.1. Considerando as explanações acima, foram recebidas no total de 8 (oito) propostas de fornecedores distintos para manutenção da solução atualmente em uso e para substituição por outra solução de outro fabricante, considerando os períodos de 12 e 36 meses de vigência, conforme **Anexo II -Mapa_Comparativo_de_preços_12_meses e Anexo III - Mapa_Comparativo_de_preços_36_meses deste Estudo Técnico Preliminar.**

11.3.2 Considerando a pesquisa de preços realizada junto a fornecedores, após o recebimento e a validação das propostas, verificou-se que os valores para manutenção da solução atualmente em uso mostram-se economicamente mais vantajosos quando comparados ao cenário de substituição da solução.

11.3.3. Quanto ao período de vigência, foi verificado que não há redução no valor da subscrição caso a contratação seja realizada por prazo superior a 12 (doze) meses, assim, para a pretendida contratação, será considerada a vigência de 12 meses.

11.3.4. Ressalta-se, ainda, que, ao compararmos a proposta de menor valor para o período de 12 (doze) meses no cenário de manutenção da solução em uso, no montante de **R$ 10.680.485,49** (dez milhões, seiscentos e oitenta mil quatrocentos e oitenta e cinco reais e quarenta e nove centavos), com a proposta de menor valor apresentada para o cenário de substituição da solução, no montante de **R$ 14.683.334,54** (quatorze milhões, seiscentos e oitenta e três mil trezentos e trinta e quatro reais e cinquenta e quatro centavos), observa-se uma diferença de **R$ 4.002.849,05** (quatro milhões, dois mil oitocentos e quarenta e nove reais e cinco centavos), o que corresponde a aproximadamente **37%** (trinta e sete por cento).

11.3.5. Dessa forma, evidencia-se a vantajosidade econômica da manutenção da solução utilizada no MS.

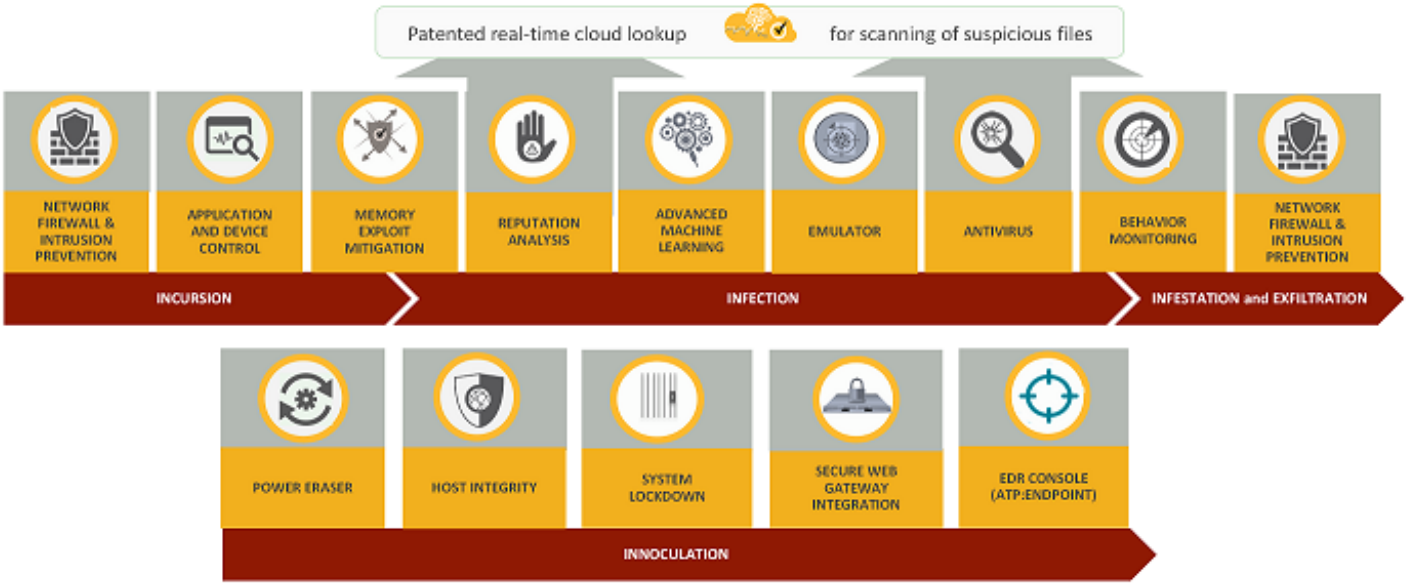
12. Descrição da solução de TIC a ser contratada

12.1. A solução de TIC a ser contratada tem por objetivo prover proteção avançada de *endpoints*, abrangendo estações de trabalho e notebooks corporativos, por meio da utilização da plataforma **Symantec Endpoint Security (Broadcom)**, a qual combina mecanismos de prevenção, detecção, resposta e controle centralizado de ameaças cibernéticas.

12.2. Trata-se de uma solução consolidada, com ampla utilização em ambientes corporativos e governamentais, oferecendo defesa multicamadas e gestão unificada de segurança em tempo real, capaz de mitigar ameaças conhecidas e desconhecidas, inclusive ataques de *ransomware*, exploração de vulnerabilidades e execução de códigos maliciosos em memória.

12.3. O Symantec Endpoint Security (SES) fornece proteção de várias camadas para impedir as ameaças, independentemente de como eles atacam os *endpoints*, gerenciada por meio de um console de nuvem unificado que fornece visibilidade das ameaças nos *endpoints* e usa diversas tecnologias para gerenciar a segurança da organização, neste caso, o Ministério da Saúde.

12.4. A mencionada solução conta com uma abordagem em camadas para a defesa, proporcionando proteção para a rede antes, durante e após um ataque, reduzindo o risco de exposição e fornecendo ferramentas para aumentar sua postura de segurança antes de qualquer ataque.



Fonte: https://techdocs.broadcom.com/br/pt_br/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/what-is-v45096464-d43e1648/how-symantec-endpoint-protection-technologies-prot-v97539434-d43e1669.html

12.5. O Symantec Endpoint Protection usa a abordagem de segurança holística para proteger o ambiente ao longo de toda a cadeia de ataque usando estas etapas: invasão, infecção, infestação, exfiltração, correção e vacinação.

12.5.1. Fase 1: Invasão

a) Proteção contra os ataques antes que eles entrem no sistema, utilizando as seguintes tecnologias:

- Prevenção contra intrusões/*firewall* (Proteção contra ameaças à rede): analisa todo o tráfego de entrada e saída e oferece proteção do navegador para bloquear essas ameaças antes que possam ser executadas no computador. O *firewall* com base em regras e a proteção do navegador protegem contra ataques na *Web*;
- Controle de aplicativos: controla o acesso a arquivos e ao registro e as permissões de execução dos processos;
- Controle de dispositivo: restringe o acesso para selecionar hardware e controla os tipos de dispositivos que podem fazer o upload ou o download de informações;
- Mitigação genérica de explorações: neutraliza explorações de dia zero, como "*Heap Spray*", a substituição de SEHOP e explorações de Java em *softwares* conhecidos não corrigidas pelos fornecedores.

12.5.2. Fase 2: Infecção

a) O Symantec Endpoint Protection usa as seguintes tecnologias para detectar e impedir ataques antes que eles infectem o sistema:

- Mitigação genérica de explorações: Detecta malware;
- Análise de reputação de arquivos (*Insight*): com base na inteligência artificial que usa a *Symantec Global Intelligence Network*. Essa análise avançada examina bilhões de ligações correlacionadas de usuários, sites e

arquivos para identificar e proteger contra *malwares* que mudam rapidamente. Ao analisar os principais atributos (como o ponto de origem de um *download* de arquivo), a Symantec pode identificar com precisão se um arquivo é bom ou ruim e atribuir uma pontuação de reputação antes que o arquivo chegue ao computador cliente;

- Aprendizado de máquina avançado: analisa os trilhões de exemplos de arquivos seguros e perigosos contidos em uma rede de inteligência global. Aprendizado de máquina avançado é uma tecnologia não assinada que pode bloquear novas variações de *malwares* antes da execução;
- Emulação de alta velocidade: detecta *malwares* ocultos usando compactadores polimorfos personalizados;
- Proteção contra *malware*: usa antivírus com base em assinaturas e heurística de arquivos para localizar e erradicar *malware* de um sistema, protegendo-o contra vírus, *worms*, cavalos de Troia, *spywares*, *bots*, *adwares* e *rootkits;*
- Análise comportamental: usa o aprendizado de máquina para fornecer proteção de dia zero, impedindo ameaças novas e desconhecidas por meio do monitoramento de cerca de 1.400 comportamentos de arquivos enquanto eles são executados em tempo real para determinar o risco dos arquivos;
- Proteção adaptável: usa o mecanismo de análise comportamental, bem como a telemetria e a experiência globais em ameaças para reduzir a superfície de ataque gerenciando comportamentos potencialmente arriscados de aplicativos confiáveis.

12.5.3. Fase 3: Infestação e exfiltração

a) A exfiltração de dados é a transferência não autorizada de dados de um computador. Ao assumirem o controle desses sistemas de destino, os invasores poderão roubar propriedade intelectual ou outros dados confidenciais. Os invasores usam as informações capturadas para análise e explorações ou fraudes futuras.

- Prevenção contra intrusões/*firewall*: bloquear as ameaças enquanto elas transitam pela rede;
- Análise comportamental: ajuda a impedir a propagação de infecções.

12.5.4. Fase 4: Correção e vacinação

a) O Symantec Endpoint Protection inclui um único console e agente que oferece proteção entre sistemas operacionais, plataformas e empresas de qualquer tamanho.

- *Power Eraser:* ferramenta que pode ser acionada remotamente e que age com agressividade contra ameaças avançadas persistentes, corrigindo malwares resistentes;
- Integridade do *host*: garante, por meio de imposição de políticas, detecção de alterações não autorizadas e condução de avaliações de danos, que os *endpoints* estejam protegidos e em conformidade. A Integridade do *host* isolará os sistemas gerenciados que não atenderem aos seus requisitos;
- Bloqueio do sistema: permite que os aplicativos (conhecidos como seguros) sejam executados ou bloqueia a execução dos aplicativos (conhecidos como perigosos);
- Integração com o *Cloud Secure Web Gateway:* usa APIs REST programáveis para possibilitar a integração com o *Secure Web Gateway* e ajudar a interromper rapidamente a propagação de infecções;
- Integração com o console do EDR: o Symantec Endpoint Protection é integrado ao Symantec EDR e foi projetado para detectar, responder e bloquear ataques direcionados e ameaças avançadas persistentes com mais rapidez ao priorizar os ataques. O recurso EDR *(Endpoint Detection and Response)* é integrado ao Symantec Endpoint Protection, o que torna desnecessária a implementação de outros agentes.

12.6. Componentes da arquitetura do Symantec Endpoint Protection

12.6.1. A arquitetura do Symantec Endpoint Protection usa três grupos funcionais de componentes. Alguns dos componentes pertencem a vários grupos porque eles são multifuncionais, conforme ilustrado na figura a seguir:

Fonte: https://techdocs.broadcom.com/br/pt_br/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/what-is-v45096464-d43e1648/architecture-components-v17119278-d43e1975.html

12.7. O Symantec Endpoint Security fornece segurança em dispositivos Windows, Mac, Linux e móveis nas seguintes fases de ataque: pré-ataque, ataque, violação e pós-ataque. A tabela a seguir exibe o tipo de implementação do Symantec Endpoint Protection no local e determina quais recursos são compatíveis:

Recurso	Descrição
Prevenção contra ataques	
Política *Antimalware*	* Chamada de política de Proteção contra vírus e *spywares*; e * Configurações da política *Antimalware.*
Política MEM	* Chamada de Mitigação de explorações da memória; e * Gerenciamento de políticas de MEM (*Memory Exploit Mitigation* - Mitigação de explorações da memória).
Política de integridade do *host*	Compatível apenas com estações de trabalho do *Windows*.
Política da Proteção de acesso a *web* e nuvem	Como configurar a política de Proteção de acesso à *web* e à nuvem.
Ataque	
Política de Comportamento do aplicativo personalizado	* Chamada de política de Controle de aplicativos; e * Gerenciamento de comportamentos do aplicativo personalizado.
Política do Controle de dispositivos	Como bloquear ou permitir um dispositivo externo usando o Controle de dispositivos.
Prevenção contra violações	
Política de *firewall*	Como gerenciar o *firewall* do Symantec Endpoint Security.
Política de prevenção contra intrusões	Introdução à prevenção contra intrusões.
Política da Proteção adaptável	* Compatível apenas com estações de trabalho do Windows; * Como bloquear ataques LOTL *(Living Off the Land)* com a Proteção adaptável.
Fraude	Compatível apenas com estações de trabalho do *Windows*.

Active Directory	Compatível apenas com estações de trabalho do *Windows*.
Content Analysis	Requer Symantec EDR local.
Resposta e correção	
Política Detecção e resposta	Requer uma assinatura do Symantec EDR local.
Outras políticas	
Política de Lista de bloqueio	* Chamada de política de exceções; * Como usar as configurações da política de Lista de bloqueio.
Política de Lista de permissão	*Chamada de política de exceções; * Como gerenciar itens negados e itens permitidos na lista central.
Política de sistema	*Várias políticas e configurações; * Inclui configurações para *LiveUpdate*, configuração do *proxy*, atualização automática do agente, proteção contra adulterações, reinicialização do cliente, senha do cliente; e * Como fazer *download* do conteúdo do *LiveUpdate* para os dispositivos.

Fonte: https://techdocs.broadcom.com/br/pt_br/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Getting-Started/what-is-v129161010-d4161e112.html

12.8. Componentes Principais da Solução

Componente	Descrição Técnica
Antivírus e *Antimalware*	Mecanismos de varredura comportamental e análise heurística para bloqueio de vírus, *spyware*, trojans e *ransomware*.
Intrusion Prevention System (IPS)	Inspeção de tráfego e prevenção de tentativas de exploração de vulnerabilidades em *endpoints*.
***Firewall* Pessoal e Controle de Aplicações**	Gerenciamento de políticas de acesso à rede e controle sobre execução de *softwares* não autorizados.
Device Control	Controle granular sobre dispositivos externos (pendrives, mídias removíveis), prevenindo vazamento de informações.
Host Integrity* e *Compliance	Monitoramento de conformidade e integridade de estações com as políticas de segurança definidas.
Endpoint Detection and Response (EDR)	Detecção de comportamentos anômalos, correlação de eventos e capacidade de resposta a incidentes de segurança.
Console Central de Gerenciamento	Interface única para administração de políticas, monitoramento, relatórios e integração com demais sistemas corporativos.
Atualizações e Inteligência de Ameaças	Integração com a base global de inteligência da Broadcom, com atualizações automáticas e contínuas de assinaturas e regras de detecção.

12.8.1 As especificações técnicas da solução de TIC encontram-se no Anexo I deste Estudo Técnico Preliminar.

12.9. Justificativa da natureza da despesa

12.9.1. Considerando a natureza dos serviços pretendidos e sua essencialidade para a continuidade das atividades institucionais, a presente contratação caracteriza-se como atividade de custeio, não se configurando como despesa de investimento.

12.9.2. Os serviços objeto da contratação possuem natureza continuada, uma vez que constituem atividade essencial e permanente para manutenção da solução de segurança destinada à proteção de endpoints em estações de trabalho, notebooks e servidores do Ministério da Saúde, contribuindo para a preservação da disponibilidade, integridade e confidencialidade dos ativos de informação.

12.9.3. Ressalta-se que o modelo de contratação por subscrição confere ao órgão exclusivamente o direito de uso da solução durante o período de vigência contratual, incluindo suporte e atualização, sem transferência de propriedade ou aquisição de licenças perpétuas passíveis de incorporação definitiva ao patrimônio público como ativo intangível.

12.9.4. A necessidade de proteção contra ameaças digitais possui caráter contínuo e ininterrupto, de modo que eventual interrupção ou descontinuidade da solução poderá acarretar impactos operacionais, financeiros, reputacionais e de conformidade regulatória, incluindo indisponibilidade de serviços essenciais, exposição a incidentes de segurança, comprometimento de informações críticas e riscos relacionados ao cumprimento da legislação aplicável de proteção de dados.

12.9.5. Dessa forma, considerando que a natureza do serviço demanda prestação contínua e superior a um exercício financeiro, justifica-se a adoção de vigência plurianual como medida necessária para assegurar a continuidade do serviço público e a manutenção dos níveis adequados de segurança do ambiente digital do Ministério da Saúde.

12.10. Justificativa para a escolha da qualificação econômico-financeira

12.10.1. A exigência de qualificação econômico-financeira visa assegurar que a futura contratada possua condições mínimas de sustentabilidade financeira e capacidade econômica para executar adequadamente o objeto contratado durante toda a vigência contratual, reduzindo riscos de descontinuidade, inadimplemento ou comprometimento da execução.

12.10.2. Considerando a natureza e a relevância dos serviços pretendidos, bem como a necessidade de garantir a continuidade operacional e o adequado atendimento das obrigações contratuais, entendeu-se necessária a adoção de requisitos de habilitação econômico-financeira compatíveis com a complexidade e o porte da contratação.

12.10.3. Os critérios estabelecidos observam os princípios da proporcionalidade, razoabilidade e competitividade, de modo a não restringir indevidamente a participação de licitantes, mas apenas verificar sua capacidade econômico-financeira para suportar os custos inerentes à execução contratual.

12.10.4. Adicionalmente, a exigência adotada encontra fundamento na legislação aplicável às contratações públicas, destinando-se exclusivamente à mitigação de riscos contratuais e à preservação do interesse público, sem criar barreiras injustificadas à ampla concorrência.

13. Estimativa de custo total da contratação

Valor (R$): 10.382.428,30

13.1. Sabe-se que, os processos administrativos de contratação deverão ser instruídos com a devida justificativa de que os preços estimados são condizentes com o praticado pelo mercado. Assim, para fins de verificação de que os preços propostos são similares aos praticados, realizou-se ampla pesquisa, conforme já apontado precedentemente neste Estudo.

13.2. Todos os resultados encontrados para dar embasamento a pesquisa deste Estudo foram analisados e os resultados compatíveis foram utilizados para compor o Mapa Estimativo de Preços e a Nota Técnica 14 - Análise da Pesquisa de Preços (SEI nº 0052593587), colacionados aos autos.

13.3. O custo estimado total da contratação, que é o máximo aceitável, é de **R$ 10.382.428,30 (dez milhões, trezentos e oitenta e dois mil, quatrocentos e vinte e oito reais e trinta centavos)**, conforme custos unitários apostos na tabela abaixo:

Item	Especificação	Part number	CATSER	Unidade de medida	Quantidade	Valor unitário	Valor total por item
1	Subscrição Symantec Endpoint Security Complete	SESC-SES-CLD-SUB	27502	Unidade	15.061	R$ 167,00	R$ 2.515.187,00
2	Subscrição Symantec Data Center Security	DCS-SRVA-SUB	27502	Unidade	353	R$ 243,78	R$ 86.054,34

3	Subscrição Symantec It Management Suíte (Symantec Altiris)	ALT-SUB	27502	Unidade	15.061	R$ 173,06	R$ 2.606.456,66
4	Subscrição Symantec Messaging Gateway Hybrid	SMG-HYB-SUB	27502	Unidade	22.826	R$ 75,13	R$ 1.714.917,38
5	Subscrição Symantec Data Loss Prevention	DLP-ES-SUB	27502	Unidade	15.061	R$ 229,72	R$ 3.459.812,92
						Valor Global	**R$ 10.382.428,30**

14. Justificativa técnica da escolha da solução

14.1. Como já mencionado neste Estudo, a atual plataforma de proteção de *endpoints* em uso no Ministério da Saúde é a *Symantec Endpoint Security (Broadcom)*, amplamente consolidada no ambiente institucional e integrada às políticas de segurança e infraestrutura tecnológica vigentes.

14.2. A solução encontra-se em pleno funcionamento, atendendo satisfatoriamente aos requisitos de proteção, controle e gestão de estações de trabalho e notebooks corporativos, exceto pelo fato de que os atuais estão próximos de seu encerramento - **Contratos nº 117 /2021, vigente até o dia 07/12/2026** e **nº 102/2022, vigente até o dia 11/11/2027.**

14.3. A substituição neste momento ignoraria dez anos de aprendizado institucional e capital intelectual acumulado, gerando riscos críticos durante a transição. É fundamental ressaltar que a substituição desta suíte tecnológica não se caracteriza como uma operação de simples execução ("plug-and-play"). Qualquer nova solução exigiria um projeto de implantação massivo, envolvendo a desinstalação manual dos agentes atuais e a instalação de novos em ambientes de missão crítica, o que impõe janelas de interrupção de serviços essenciais. Existem custos ocultos vultosos: a necessidade de reconstruir todas as políticas de segurança e o risco de exposição do órgão durante o vácuo operacional da migração. O suposto ganho econômico no licenciamento é neutralizado pelo custo de reimplantação e pela perda de maturidade nos processos do suporte e do SOC.

14.4. A Symantec/Broadcom oferece uma plataforma de proteção multicamadas, contemplando antivírus, *antimalware*, controle de dispositivos, prevenção de intrusões (IPS) e gerenciamento centralizado de políticas de segurança. Sua arquitetura híbrida - com componentes locais e gerenciamento em nuvem - permite amplo controle sobre os *endpoints*, mantendo visibilidade e conformidade com as diretrizes de segurança institucional.

14.5. A escolha da referida solução apresenta:

14.5.1. Alta compatibilidade com o parque tecnológico existente no Ministério da Saúde;

14.5.2. Integração já estabelecida com sistemas de diretórios *(Active Directory)* e mecanismos de autenticação corporativa;

14.5.3. Políticas e perfis de segurança customizados, ajustados às diferentes unidades organizacionais;

14.5.4. Estabilidade operacional comprovada, sem registros de falhas críticas ou incompatibilidades significativas;

14.5.5. Suporte técnico ativo junto ao fornecedor, com atualizações de assinaturas, *patches* e correções regulares;

14.5.6. Continuidade operacional, sem impacto aos usuários, evitando interrupções em atividades críticas, especialmente em ambientes de grande escala e alta disponibilidade;

14.5.7. Preservação de investimentos realizados, uma vez que a manutenção do ambiente evita custos adicionais de migração, reconfiguração e treinamento;

14.5.8. Baixo risco técnico, tendo em vista que, por se tratar de um ambiente estável e maduro, a manutenção apresenta baixo risco operacional, mantendo controles de segurança já testados, consolidados e auditados;

14.5.9. A solução atual permanece aderente às políticas internas de segurança da informação, bem como às normas de governança (ISO/IEC 27001, LGPD e diretrizes do Governo Federal para segurança cibernética); e

14.5.10. A Broadcom mantém atualizações de assinaturas, correções de vulnerabilidades e suporte técnico especializado, garantindo a continuidade da proteção contra novas ameaças.

14.6. Pela análise técnica, a renovação da suíte Broadcom/Symantec é a estratégia que melhor assegura a resiliência cibernética e a continuidade operacional do Ministério da Saúde. A solução atual entrega os requisitos modernos de nuvem, mantendo a estabilidade de um parque complexo, preservando o conhecimento técnico acumulado em mais de uma década, em conformidade com o PPSI e as diretrizes do TCU.

14.7. Por fim, a manutenção da atual solução se mostra tecnicamente adequada e economicamente racional, garantindo continuidade, estabilidade e segurança operacional, sem prejuízo aos níveis de proteção atualmente implementados. A decisão permite que a instituição preserve investimentos, mantenha conformidade regulatória e reduza riscos de transição, assegurando a eficiência dos mecanismos de defesa cibernética existentes.

14.8. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

14.8.1. A contratação será realizada em grupo único, pois se trata de uma solução de segurança (subscrições) para proteção de endpoints com características e funcionalidades semelhantes, ou seja, possuem mesma natureza.

14.8.2. A opção pelo não parcelamento da solução fundamenta-se em aspectos técnicos, operacionais e de segurança da informação, considerando que o objeto pretendido caracteriza-se como uma solução integrada e indivisível, cujo pleno funcionamento depende da atuação conjunta e coordenada de todos os seus componentes.

14.8.3. O fracionamento da contratação em múltiplos objetos ou fornecedores distintos poderia acarretar: Risco à segurança da informação, decorrente da fragmentação das políticas de proteção, da ausência de correlação centralizada de eventos e da dificuldade de resposta coordenada a incidentes; Perda de eficiência operacional, em razão da necessidade de integração entre soluções heterogêneas, com diferentes arquiteturas, consoles de gestão e modelos de atualização; Aumento da complexidade administrativa e contratual, com maior esforço de fiscalização, gestão de múltiplos contratos e responsabilização difusa em caso de falhas ou incidentes; Risco de incompatibilidade tecnológica, que pode comprometer a interoperabilidade entre os módulos de proteção de endpoints, servidores, correio eletrônico, gestão de ativos e prevenção de vazamento de dados.

14.8.4. Além disso, a natureza das ameaças cibernéticas atuais exige visibilidade unificada, inteligência compartilhada e resposta orquestrada, o que somente é viável por meio de uma solução que ofereça integração nativa entre seus componentes, sob gestão centralizada.

14.8.5. No que se refere aos princípios da competitividade, proporcionalidade e razoabilidade, destaca-se que a opção pelo não parcelamento não se destina a restringir indevidamente a competição, mas sim a preservar a integridade técnica do objeto, sendo compatível com o mercado de soluções corporativas de segurança, que usualmente oferece plataformas integradas e escaláveis.

14.8.6. Dessa forma, conclui-se que o não parcelamento da solução é tecnicamente justificado, economicamente vantajoso e juridicamente adequado, atendendo aos princípios previstos no art. 11 da Lei nº 14.133/2021 e contribuindo para a obtenção do melhor resultado para a Administração.

15. Justificativa econômica da escolha da solução

15.1. A manutenção da solução de proteção de *endpoints* atualmente utilizada (Symantec/Broadcom) apresenta-se como uma alternativa economicamente vantajosa diante dos custos e riscos inerentes à substituição por nova plataforma. O contrato vigente contempla infraestrutura implantada, licenciamento ativo e equipe já capacitada, o que reduz substancialmente a necessidade de novos investimentos.

15.2. Sob uma ótica do racional econômico, a análise comparativa entre o custo de manutenção da solução atual e o custo potencial de migração demonstra que a continuidade com a Symantec/Broadcom representa melhor custo-benefício no curto e médio prazos, considerando:

15.2.1. Aproveitamento dos investimentos existentes;

a) O Ministério da Saúde já dispõe de infraestrutura de servidores, consoles de gestão e políticas configuradas especificamente para a solução atual;

b) A manutenção evita despesas com reinstalação, reconfiguração e revalidação de políticas;

c) Preserva o investimento realizado em capacitação técnica da equipe responsável pela administração da plataforma.

15.2.2. Eliminação de custos de transição;

a) A substituição da solução implicaria em custos adicionais, como: aquisição de novas licenças e subscrições; serviços profissionais de migração e integração; horas técnicas de implantação, customização e testes de compatibilidade; treinamento e capacitação de equipes técnicas e usuários finais;

b) Tais custos indiretos poderiam elevar significativamente o valor total da substituição, mesmo que o licenciamento inicial da nova solução fosse competitivo.

15.2.3. Previsibilidade orçamentária;

a) A manutenção da solução atual permite previsão orçamentária estável, uma vez que os valores de renovação e suporte são, em sua maior parte, tabelados;

b) Isso favorece o planejamento financeiro e a continuidade do serviço, sem necessidade de dotação extraordinária para migração e treinamentos.

15.2.4. Redução de riscos financeiros;

a) A manutenção da atual solução minimiza riscos de desperdício de recursos públicos, evitando a aquisição de tecnologia que possa demandar retrabalho, incompatibilidades ou custos imprevistos de adequação;

b) Além disso, reduz-se o risco de interrupção de serviço e eventuais prejuízos operacionais que poderiam gerar impactos econômicos indiretos.

15.3. A relação custo-benefício da manutenção da Symantec/Broadcom é favorável, pois garante:

- Proteção corporativa em nível satisfatório, com desempenho comprovado;
- Baixo custo de operação, uma vez que a equipe e infraestrutura já estão estabelecidas;
- Despesas previsíveis, limitadas à renovação das subscrições de suporte e atualizações;
- Menor custo total de propriedade (TCO) quando comparado à aquisição e implantação de uma nova solução.

15.4. Pelo exposto, a manutenção da solução Symantec/Broadcom demonstra-se economicamente justificável e financeiramente prudente, por preservar os investimentos realizados, evitar gastos adicionais com migração e assegurar previsibilidade orçamentária, conforme demostrado no item 11. Análise comparativa de custos (TCO).

15.5. A opção atende aos princípios de economicidade, eficiência e continuidade do serviço público, conforme orientações da Lei nº 14.133/2021 (Nova Lei de Licitações e Contratos).

16. Benefícios a serem alcançados com a contratação

16.1. Resultados e benefícios a serem alcançados:

16.1.1. Consolidação da segurança da informação relacionada aos aspectos de disponibilidade, confidencialidade e integridade das informações;

16.1.2. Proteção e garantia da disponibilidade e integridade das informações nos *endpoints* e redução dos riscos de ameaças maliciosas;

16.1.3. Redução de custos com migração e treinamento;

16.1.4. Alcance do suporte oficial do fabricante para os casos de correções de segurança e de resolução de problemas na utilização dos *softwares*;

16.1.5. Atualização do ambiente computacional do MS, com a disponibilização de subscrições atualizadas;

16.1.6. Redução do tempo de detecção e resposta a incidentes;

16.1.7. Visibilidade centralizada e gestão unificada;

16.1.8. Aprimoramento contínuo e escalabilidade; e

16.1.9. Atendimento às diretrizes da PPSI 2.0 e conformidade com a LGPD.

17. Providências a serem Adotadas

17.1. A área requisitante, em conjunto com as áreas competentes, deverá:

17.1.1. Elaborar a minuta do Termo de Referência, com base nas especificações técnicas já validadas neste ETP; e

17.1.2. Assegurar a disponibilidade orçamentária, conforme previsão no PCA 2026 e no PDTIC vigente.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

A viabilidade desta contratação encontra respaldo nos fundamentos expostos no presente Estudo Técnico Preliminar, sendo que as análises realizadas demonstram, de forma clara e objetiva, a compatibilidade da solução proposta com as necessidades e objetivos do Ministério da Saúde.

A escolha da modalidade e a forma de contratação visam assegurar a obtenção da melhor solução técnica e econômica, em consonância com os princípios da legalidade, eficiência e economicidade, previstos na legislação vigente.

Assim, com base nas justificativas apresentadas e em observância ao interesse público, conclui-se pela viabilidade da contratação, a qual está devidamente fundamentada nos elementos técnicos e legais contidos neste documento.

19. Responsáveis

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

Despacho: Afirmo estar ciente da minha responsabilidade como membro da equipe responsável pelo planejamento da contratação como Integrante Requisitante.

RAMON MORENO DE MATOS VIEIRA

Integrante Requisitante

Assinou eletronicamente em 16/06/2026 às 18:06:17.

Despacho: Afirmo estar ciente da minha responsabilidade como membro da equipe responsável pelo planejamento da contratação como Integrante Técnico.

MARCELO DIAS DE SA

Integrante Técnico

Assinou eletronicamente em 15/06/2026 às 13:58:51.

Despacho: Aprovo o presente Termo de Referência como Autoridade Competente e Autoridade Máxima da Área de TIC, bem como declaro a adequação dos estudos realizados aos ditames da IN SGD n° 94/2022.

ROBSON WILLIAN DE MELO MATOS

Autoridade competente

Assinou eletronicamente em 30/06/2026 às 10:00:25.